

MATH 494: HONORS ALGEBRA II

CONTENTS

1. January 4, 2017	1
2. January 6, 2017	3
3. January 9, 2017	7
4. January 11, 2017	9
5. January 13, 2017	11
6. January 18, 2017	12
7. January 20, 2017	14
8. January 23, 2017	15
9. January 25, 2017	16
10. January 27, 2017	17
11. January 30, 2017	19
12. February 1, 2017	20
13. February 3, 2017	21
14. February 6, 2017	22
15. February 8, 2017	24
16. February 10, 2017	25
17. February 13, 2017	27
18. February 15, 2017	28
19. February 17, 2017	29
20. February 20, 2017	30
21. February 22, 2017	32
22. February 24, 2017	33

1. JANUARY 4, 2017

Rings

Definition 1.1.

a) A **ring** is a tuple $(R, +, \cdot, 0)$ where:

- R is a set
- $0 \in R$
- $+, \cdot : R \times R \rightarrow R, \quad (a, b) \mapsto a + b, a \cdot b$

subject to:

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

- b) A **ring with unity** is a tuple $(R, +, \cdot, 0, 1)$, where $(R, +, \cdot, 0)$ is a ring, and $1 \in R$ is subject to $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.
- c) A ring $(R, +, \cdot, 0)$ is called **commutative** if $ab = ba$ for all $a, b \in R$.
- d) A **field** is a commutative ring with unity $(R, +, \cdot, 0, 1)$ such that $(R \setminus \{0\}, \cdot, 1)$ 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 $(R \setminus \{0\}, \cdot, 1)$ 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
($\text{supp}(f) = \overline{\{x \in \mathbb{R} \mid f(x) \neq 0\}}$) is a commutative ring without unity
- $R = \{\star\}, 0 = 1 = \star$ is the **zero ring**.

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

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

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

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

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

Fact 1.5.

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

Proof.

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

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

Definition 1.6. Let R, S be rings. A **morphism** $\phi : R \rightarrow S$ is a map of sets $\phi : R \rightarrow S$ satisfying

- $\phi(a + b) = \phi(a) + \phi(b)$
- $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$
- $\phi(1) = 1$

Example. $\phi : \mathbb{Z} \rightarrow \mathbb{Z} \ u \mapsto 0$ 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 $\phi : \mathbb{Z} \rightarrow R$. 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.

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

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

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

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 $\varphi : R \rightarrow S$ 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 $0 \in \ker(\varphi)$. 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?

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

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

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

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

- $p(1_R) = 1_{R/I}$
- The following diagram to commute

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

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

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

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

$$(a' + I)(b' + I) = (a' \cdot b') + I = ((a + i) \cdot (b + j)) + I = (a \cdot b + a \cdot j + b \cdot i + i \cdot j) + I = a \cdot b + I$$

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

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

Remark. $\ker(p) = I$

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

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

commutes. Moreover, $\bar{\varphi}$ 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 $\bar{\varphi}$.

(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 $\bar{\varphi}$ 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 $\bar{\varphi}$. 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

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

as we have that $\varphi(i) = 0$ for all $i \in I$ (since $I \subset \ker(\varphi)$). We finally verify the injective biconditional. Assume $\bar{\varphi}$ is injective. We already have that $I \subset \ker(\varphi)$. Now, since $\bar{\varphi}$ 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 $\bar{\varphi}$, 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 $\ker(\bar{\varphi})$. 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 $\ker(\bar{\varphi}) = I$. Since the kernel of $\bar{\varphi}$ is trivial, we have that $\bar{\varphi}$ is injective.

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

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

□

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 Exclusive). 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 $\varphi : R \rightarrow S$ 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 shown 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 $F \setminus \{0\}$ 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

$$I \text{ is a maximal ideal} \xLeftrightarrow{\text{v}} R/I \text{ is a field} \xRightarrow{\text{vi}} R/I \text{ is a domain} \xLeftrightarrow{\text{ii}} I \text{ is prime.}$$

\square

3. JANUARY 9, 2017

Definition 3.1. Let R be a domain. The canonical morphism $\mathbb{Z} \rightarrow R$ 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 or $p = 0$. We call p the **characteristic** of R .

Example.

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

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 $J_0 \in \mathcal{M}$. \square

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. \square

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 $\varphi_1 : R \rightarrow S_1, \varphi_2 : R \rightarrow S_2$, we get a unique morphism $\varphi_1 \times \varphi_2 : R \rightarrow S_1 \times S_2$.

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

$$p : R \rightarrow R/I_1 \times R/I_2 \times \dots \times R/I_n$$

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

$$\bar{p} : R/(I_1 \cap I_2 \cap \dots \cap I_n) \rightarrow R/I_1 \times R/I_2 \times \dots \times R/I_n$$

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

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 $R/I_1 \cap I_2 \cap \cdots \cap I_n$ and also induces an injective ring morphism $\bar{p} : R/I_1 \cap \cdots \cap I_n \rightarrow R/I_1 \times \cdots \times R/I_n$.

Claim. \bar{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 $u_1 \in 1 + I_1$, 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 $(x_1, \dots, x_n) \in R/I_1 \times \cdots \times R/I_n$. 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 $u_1 r_1 + u_2 r_2 \cdots u_n r_n$, 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 \bar{p} . This proves surjectivity. \square

Thus, we have that \bar{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 $I_1 \cap I_2 \subset I_1 \cdot I_2$.

Now, for general n . By the inductive hypothesis, we have that $I_1 \cap I_2 \cdots I_n \subset (I_1 \cdots I_{n-1}) \cap I_n$. 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, $i : R \rightarrow K$ an injective morphism such that if (j, L) is another such pair, there exists a morphism $l : K \rightarrow L$ such that $j = l \circ i$, which is to say that the following diagram commutes.*

$$\begin{array}{ccc} & R & \\ i \swarrow & & \searrow j \\ K & \xrightarrow{l} & L \end{array}$$

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

$$\begin{array}{ccc} & R & \\ i \swarrow & & \searrow i' \\ K & \xrightarrow{\phi} & K' \end{array} \quad \text{commutes.}$$

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 $l : K \rightarrow K'$. Do it the other way to get $l' : K' \rightarrow K$.

Claim. $l \circ l' = \text{id}_{K'}$, $l' \circ l = \text{id}_K$

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

$$\begin{array}{ccc} & R & \\ i \swarrow & & \searrow i \\ K & \xrightarrow{l' \circ l} & L \end{array}$$

$$\begin{array}{ccc} & R & \\ i \swarrow & & \searrow i \\ K & \xrightarrow{i \circ \text{id}_K} & L \end{array} \quad \text{commute.}$$

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 2.6, 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, $n_1 d_3 = n_3 d_1$. Either way, we are done. \square

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

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

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

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

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

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 $l : K \rightarrow L$ 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. \square

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 $a_n T^n + a_{n-1} T^{n-1} + \dots + a_0, a_i \in R$.

2) Given $P(T) = a_n T^n + \dots + a_0, Q(T) = b_n T^n + \dots + b_0$ define

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

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

where

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

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

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

Fact 4.4. $(R[T], +, \cdot, 0, 1)$ is a ring. Moreover $R \rightarrow R[T], r \rightarrow \text{constant polynomial } r$ 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 $R \rightarrow R$ by $r \mapsto P(r) = a_n r^n + \dots + a_0$. 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 $\phi : R \rightarrow S$ be a morphism and let $s \in S$. There exists a unique morphism $\phi_s : R[T] \rightarrow S$ 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 $\phi_s(a_n T^n + \dots + a_0)$ must equal $\phi(a_n)s^n + \dots + \phi(a_0)$. This proves uniqueness and existence (upon checking that this is a morphism). \square

Example.

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

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

Proposition 5.2. Let $P = a_n T^n + \dots + a_0 \in R[T]$. We have $P \in R[T]^\times$ iff $a_0 \in R^\times$ and a_1, \dots, 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 4.6, $0 = \deg(1) = \deg(PQ) = \deg(P) + \deg(Q)$ (R is a domain so the leading coefficient of P (alternatively Q) is not a zero divisor). Thus $\deg(P), \deg(Q) = 0$. Thus $a_1, \dots, a_n = 0$ 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 $a_1, \dots, a_n = 0_{R/\mathcal{P}}$ and thus $a_1, \dots, a_n \in \mathcal{P}$. Since this holds for all \mathcal{P} , by HW we have that a_1, \dots, a_n are nilpotent. \square

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 5.1 with $S = R[T]$, $\phi : R \hookrightarrow R[T]$, $s = T + r$ to get a morphism $R[T] \rightarrow R[T]$. 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 $Q(T) = b_n T^n + \dots + b_1 T$ 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 $R[T] \rightarrow R[T]$ 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 $R[T] \rightarrow R[T]$ which “replaces every T with $T - r$.” In particular, the preimage of $Q(T) = b_n T^n + \dots + b_1 T$ is $b_n(T - r)^n + \dots + b_1(T - r)$. \square

Proposition 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 $D = d_n T^n + \dots + d_0$ and $Z = z_m T^m + \dots + z_0$ 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 by (4.6) $\deg(D) > \max(\deg(Z'), \deg(Z)) \geq \deg(Z' - Z) = \deg((Q - Q')D) = \deg(Q - Q') + \deg(D)$ (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. (This is Lemma 3 from Jan. 13) (5.3) Given $P \in R[T], r \in R$, then $P(r) = 0 \Leftrightarrow (T - r) \mid P$.

Proposition. (This is Proposition 4 from Jan. 13) (5.4) 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 5.3 which utilizes 5.4.

Proof. As per 5.4, 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 6.0. Let $P \in R[T], r \in R$. Define **the multiplicity of r in P** by $\max\{n \in \mathbb{N} : (T - r)^n \mid P\}$.

Corollary 6.1. 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 5.3, $P = (T - r) \cdot Q(T)$ 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.

□

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

Proposition 6.3. 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 $c, r_1, \dots, r_n \in k, m_1, \dots, m_n \in \mathbb{N}$.

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

Definition 6.4. Define $\mathbf{R}[T_1, \dots, T_n]$ recursively as $(R[T_1, \dots, T_{n-1}])[T_n]$. More concretely: a **monomial** in T_1, \dots, 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, \dots, T_n with coefficients in R is an R -linear combination of monomials; the set of all polynomials in T_1, \dots, T_n is $R[T_1, \dots, T_n]$.

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

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

Fact 6.5. Given a ring morphism $\phi: R \rightarrow S, s_1, \dots, s_n \in S$, there exists a unique ring morphism

$$\phi_{s_1, \dots, s_n}: R[T_1, \dots, T_n] \rightarrow S$$

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

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

Definition 6.6.

- The image of ϕ_{s_1, \dots, s_n} is called the **R -subalgebra of S generated by s_1, \dots, s_n**
- s_1, \dots, s_n are called **algebraically independent** provided that ϕ_{s_1, \dots, 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 ϕ_{s_1, \dots, s_n} we have

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

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 6.7. 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 6.8. 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 $c = b^{-1} \Leftrightarrow b \in R^\times$. \square

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 6.9. 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

Proposition 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 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 **Principal 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 $a_0 = a_1 a_2 a_3 \dots$ 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

$$(a_0) \subsetneq (a_1) \subsetneq \dots$$

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 $H : R \setminus \{0\} \rightarrow \mathbb{N}$ 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.

Proposition 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 7.6. If F is a field, $F[T]$ is a PID, and hence a UFD.

Definition 7.7. 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 7.8. (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 $R[T] \rightarrow (R/(p))[T]$.

But $R/(p)$ is a domain by 2.8, and thus, by 4.6, 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. \square

8. JANUARY 23, 2017

Recall: $P \in R[T]$ is primitive if $a \mid P \implies a \in R^\times$. Lemma 7.8 (Gauss): P, Q primitive $\implies P \cdot Q$ primitive. R is a UFD, F is its 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 $n = \epsilon n_1 \dots n_k, d = \mu v_1 \dots v_k$ into irreducibles. We may assume $n_i \sim v_j$ for i, j . Then $\mu v_1 \dots v_k Q = \epsilon n_1 \dots n_k P$. So $v_1 | n_1 \dots n_k a_i$ for all i , where $P(T) = a_n T^n + \dots + a_0$. Since v_1 is prime, and n_i are irreducible, and $v_1 \approx u_1, \dots, u_k$, so $v_1 | a_i$ for all i . This contradicts primitivity of P . \square

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 (5.2). Say WOLOG $S = R[T] \cap F^\times = R \setminus \{0\}$. Then $S^{-1}P = Q$. By 8.1, $S^{-1} \in R$. 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 $F[T]$. $P = c \cdot \tilde{Q}_1, \dots, \tilde{Q}_n, c \in F^\times, \tilde{Q}_i \in F[T]$ irreducible. By 8.3, write $\tilde{Q}_i = c_i \cdot Q_i$ with $c_i \in F^\times, Q_i \in R[T]$ primitive. Thus $P = c \cdot c_1 \dots c_n \cdot Q_1 \dots Q_n$. By Gauss Lemma (7.8), $Q_1 \dots Q_n$ is primitive, so by 8.1, $a \in R$. Factor $a = \epsilon n_1 \dots n_k$ in R .

Remark: This shows in particular, that (1)+(2) are all the irreducible elements in $R[T]$. Uniqueness of factorization Let $\epsilon n_1 \dots n_k P_1 \dots P_n = \mu v_1 \dots v_l Q_1 \dots Q_m$ 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 8.1 to $P_i = c_i P_i Q_i$ 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 $\epsilon n_1 \dots n_k = \mu \frac{Q_1 \dots Q_n}{P_1 \dots P_n} \cdot v_1 \dots v_l$ and uniqueness in R gives us $k = l$ and $n_i \sim v_i$ after reordering. \square

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. \square

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 8.3, $\tilde{S} = aS, a \in F^\times$. $S \in R[T]$ primitive. So $Q = aPS$. By Gauss lemma (7.8), PS is primitive. By 8.1, $a \in R$, then $\tilde{S} = aS \in R[T]$. \square

9. JANUARY 25, 2017

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

Proof. Suppose not. By Thm 2 last time we have that P is not irreducible in $R[T] \implies P = Q \cdot S$ where $Q, S \in R[T]$. Let $\tilde{P}, \tilde{Q}, \tilde{S}$ be images in $(R/(P))[T]$. Write $Q(T) = b_m T^m + \dots + b_0, S(T) = c_j T^j + \dots + c_0$. Then $\tilde{P}(T)(= \tilde{a}_n T^n) = \tilde{Q}(T)(= \tilde{b}_k T^k) \cdot \tilde{S}(T)(= \tilde{c}_j T^j)$ with $k + j = n$ since $R/(P)$ is a domain since P is prime). Then $p|b_0, p|c_0 \implies p^2|a_0 = b_0 c_0$ which is a contradiction. \square

Cyclotomic Polynomials:

Definition 9.2. For $n \in \mathbb{N}$, the n th cyclotomic polynomial is $\Phi_n(T) = \prod_{\gcd(k,n)=1, k=1}^n (T - e^{2\pi i k/n})$.

Proposition 9.3. Φ is monic and has integer coefficients.

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

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

$k < n \implies k = n : T^n - 1 = \prod_{k=1}^n (T - e^{2\pi i k/n}) = \prod_{d|n} \Phi_d(T)$. By induction, $\Phi_d \in \mathbb{Z}[T]$ and monic for $d|n, d \neq n$. In particular, these Φ_d are primitive, so Gauss lemma (7.8) implies that $\prod_{d|n, d \neq n} \Phi_d =: P$ is

primitive. $T^n - 1 = \Phi_n(T) \cdot P(T)$ in $\mathbb{C}[T]$. So $P|T^n - 1$ in $\mathbb{C}[T] \implies P|T^n - 1$ in $\mathbb{Q}[T]$. By 8.4, $P|T^n - 1$ in $\mathbb{Z}[T]$. \square

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

Proof. $T^p - 1 = \Phi_1 \cdot \Phi_p = (T - 1) \cdot \Phi_p$ and $T^p - 1 = (T - 1)(T^{p-1} + T^{p-2} + \dots + 1) \implies \Phi_p = T^{p-1} + \dots + 1$. 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 $\mathbb{Z}[T] \longrightarrow \mathbb{Z}[T]$ 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 $Q(T) = a_{p-1}T^{p-1} + \dots + a_0$, p does not divide $a_{p-1}, p|a_{p-2}, \dots, a_0$. But $a_0 = Q(0) = \Phi_p(1) = p$. Apply Eisenstein (9.1). \square

Adjoining Elements:

Let R be a ring. We want to add a new element s , subject to some relation $a_n s^n + \dots + a_n = 0$ 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 $P \in R[T], P(T) = a_n T^n + \dots + a_0, S = R[T]/(P), s = \text{image of } T \text{ in } S$. 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 \mathbb{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 $[L : k] \stackrel{\text{def}}{=} \dim_k(L)$.¹

Fact 10.2. *If k_1, k_2 are subfields 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 $1 + \dots + 1$, 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 .

Proposition 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.*

¹Debacker 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.

Proof. Let $0 \neq a \in L$. The map $a \cdot : L \rightarrow L$ 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. \square

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

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

Proposition 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 $\{e_1, \dots, e_n\}$ and $\{f_1, \dots, f_m\}$ be, respectively, bases for E/k and F/k . Then the set $\{e_i \cdot f_j : i \in \{1, \dots, n\}, j \in \{1, \dots, m\}\}$ 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 10.4 above, we have that EF is a field. \square

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

- (i) Spanning: given $x \in V$ we may write $x \in \lambda_1 v_1 + \dots + \lambda_n v_n$ for $\lambda_i \in L$, with each $\lambda_i = \mu_{i,1} \ell_1 + \dots + \mu_{i,m} \ell_m$. 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 .

\square

Corollary 10.8. If $M/L/k$ is a tower of finite extensions, then $[M : k] = [M : L] \cdot [L : k]$.

Definition 10.9. 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 $\text{ev} : k[T] \rightarrow L$, $p \mapsto p(a)$ 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 $k(T)^2$ 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 10.10. 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) $a \cdot : L \rightarrow L$.

²This notation was established on homework: $k(T)$ is the set of rational functions with coefficients in k .

11. JANUARY 30, 2017

Proposition 11.1. *Let L/K be a field extension, $a \in L$ algebraic over K . Then,*

- $M_{a,K} \in k[T]$ is irreducible
- $K[T]/(M_{a/K})$ is isomorphic to $K(a) \subset L$
- The images of $1, T, \dots, T^{n-1}$ in $K[T]/(M_{a/K})$ are a basis of this K -vector space.
- $[K(a) : K] = \deg(a/K) = n$

Proof. By definition of $M_{a/K}$ the evaluation $ev : k[T] \rightarrow L$ gives an injection from $K[T]/(M_{a/K}) \rightarrow K(a)$. Since $K(a)$ is a domain, so is $K[T]/(M_{a/K})$. By 2.8, this means $(M_{a/K})$ is prime. this means that $M_{a/K}$ is prime, so $M_{a/K}$ is irreducible by 6.8

Now we show the images of $1, \dots, T^{n-1}$ in $K[T]/(M_{a/K})$ generate the space. (Pranav Exclusive) It is enough to show that they generate T^n , as for any higher dimensional coset, by division algorithm we can reduce to a coset of $(M_{a/K})$ with degree less than $\deg(a/K)$, which is then definitionally generated by $1, \dots, T^{n-1}$. If $M_{a,K}(T) = T^n + a_{n-1}T^{n-1} + \dots + a_0$, Then $T^n = -a_{n-1}T^{n-1} - \dots - a_0$ They are also linearly independent. If not, let $b_{n-1}T^{n-1} + \dots + b_0 = 0$ be a non-trivial relation. Then $Q(T) = b_{n-1}T^{n-1} + \dots + b_0 \in K[T]$ lies in $(M_{a,k})$ as it is in the kernel of the quotient map. We thus have that $M_{a,k} \mid Q$. This contradicts that $\deg(Q) < \deg(M_{a,k})$

Now we know that $K[T]/(M_{a,K})$ is a domain, containing K and is finite dimensional over K , so by 10.4, $K[T]/(M_{a,k})$ is a field. This implies that $K[T]/(M_{a/K}) \rightarrow K(a)$ is surjective as the image in $K(a)$ is now a field that contains K and a and because $K(a)$ is the smallest such field. \square

Proposition 11.2. *Let L/K be an extension, $a \in L$. The following are equivalent.*

- i) a is algebraic over K
- ii) $[K(a) : K] < \infty$
- iii) There is an intermediate field $L/E/K$, finite over K , containing a

Proof. i) \Rightarrow ii): This comes from the above proposition (11.1), final condition.

ii) \Rightarrow iii): Just let E be $K(a)$.

iii) \Rightarrow i): Since E/K is finite, the set of powers $1, a, a^2, \dots$ cannot be linearly independent over K . Thus, there are $n \in \mathbb{N}$ and $b_0, b_1, \dots, b_n \in K$ such that $b_n a^n + \dots + b_0 = 0$ Put $P(T) = b_n T^n + \dots + b_0 \in K[T]$. Then $P(a) = 0$, so a is algebraic over K , as desired. \square

Corollary 11.3. *Let L/K be an extension, $a, b \in L$ algebraic over K . Then*

- $a + b, a \cdot b$ are algebraic over K . $\deg(a + b), (a \cdot b) \leq \deg(a) \cdot \deg(b)$
- $a \neq 0$ a^{-1} is algebraic over K and $\deg(a^{-1}) = \deg(a)$

Proof. By above proposition (11.2), $K(a)$ and $K(b)$ are finite over K .

Now, $a + b, a \cdot b \in K(a) \cdot K(b)$ and $[K(a) \cdot K(b) : K] \leq [K(a) : K] \cdot [K(b) : K]$.

By 10.6 $a + b$, and $a \cdot b$ are algebraic over K . Note that $a^{-1} \in K(a)$ so $K(a^{-1}) = K(a)$ \square

Definition 11.4. An extension L/K is called **algebraic**, if all $a \in L$ are algebraic over K .

Corollary 11.5. *If L/K is finite, then it is algebraic, and $\deg(a, K) \mid [L : K]$, for any $a \in L$.*

Proof. 11.2 and 10.8 \square

Remark. $a \in L$ is algebraic over $K \iff K(a)/K$ is algebraic.

Remark. There exist infinite algebraic extensions.

12. FEBRUARY 1, 2017

Proposition 12.1. *Let $M/L/K$ be a tower of extensions.*

- 1) *If M/K is algebraic, then M/L is algebraic.*
- 2) *If M/L and L/K are algebraic, so is M/K .*

Proof. Of 1). Let $a \in M$. There exist $P \neq 0 \in K[T]$ such that $P(a) = 0$. But P can be viewed as an element of $L[T]$.

Of 2). Let $a \in M$. Since a is algebraic over L , there is $P \neq 0 \in L[T]$ such that $P(a) = 0$. $P(T) = a_n T^n + \dots a_0$, $a_i \in L$. Each a_i is algebraic over K , thus $[K(a_1, \dots, a_n) : K] < \infty$ by 11.2.

(This is implicitly inducting on that proposition, which said extending by a single element is still finite).

Now, $P \in K(a_1 \dots a_n)[T]$, so a is algebraic over the field $K(a_1, \dots, a_n)$. Thus, we have that (again by 11.2) that $[K(a_1, \dots, a_n, a) : K(a_1, \dots, a_n)] < \infty$. By 10.8, $[K(a_1, \dots, a_n, a) : K] = [K(a_1, \dots, a_n, a) : K(a_1, \dots, a_n)] \cdot [K(a_1, \dots, a_n) : K] < \infty$. Thus, by 11.2, M is algebraic. \square

Proposition 12.2. *Let $P \neq 0 \in K[T]$. There exists a finite extension L/K and $a \in L$ such that $P(a) = 0$.*

Proof. Let Q be an irreducible factor of P . Let $L = K[T]/(Q)$, $a = \text{image of } T$. Then $P(a) = 0$, as by coset operations this is exactly $P + (Q) = (Q) = 0$ in this quotient space. Since Q is irreducible, it is prime (as $K[T]$ is a UFD). So, L is a domain by 2.8. By 10.4, the set $1, T, \dots, T^{n-1}$ is a basis for the K -vector space. \square

Remark. Same is true for $P_1, \dots, P_n \in K[T]$ by inducting on n .

Corollary 12.3. *Let $P \in K[T]$. There exists a finite extension L/K $a_1 \dots a_k \in L$ distinct, $m_1 \dots m_k \in \mathbb{N}$ nonzero $c \in K$ such that*

$$P(T) = c(T - a_1)^{m_1} \dots (T - a_k)^{m_k}$$

Proof. Induct on above proposition (12.2) and 5.3. \square

Theorem 12.4. *Let K be a field. There exists an algebraically closed extension L/K .*

Lemma 12.5. *Let K be a field. There exists an extension L/K such that for every $P \in K[T] \setminus K$ there is $a \in L$ with $P(a) = 0$.*

Proof. Let $S \in K[T] \setminus K$. Let $R = K[T_p \mid p \in S]$ (We construct polynomials with variables indexed by the set S . Thus, each polynomial gets an associated variable in this larger polynomial ring). Let I be the ideal generated by $\{P(T_p) \mid p \in S\}$. For example, if $P = T^2 + 1$, then we consider $T_{T^2+1}^2 + 1$ as one generator of this ideal). Now, we do this for every polynomial in $K[T] \setminus K$.

Claim: $I \neq R$.

Proof. Assume that $I = R$. Then there are $r_1, \dots, r_n \in R$, $P_1, \dots, P_n \in S$ such that

$$1 = \sum r_i P_i(T_{P_i})$$

By 12.2, there is a finite extension L'/K and $a_{P_1}, \dots, a_{P_n} \in L'$ such that $P_i(a_{P_i}) = 0$. For $P \in S$ not among the P_1, \dots, P_n , choose $a_P \in L'$ arbitrarily. We get a map $f : S \rightarrow L'$ that sends $P \rightarrow a_P$.

There exists a unique morphism $\phi : R \rightarrow L'$ such that $\phi(T_P) = f(P)$ (This is from homework on the

construction of the polynomials of too many variables). But,

$$\begin{aligned}\varphi(1) &= \varphi\left(\sum r_i P_i(T_{P_i})\right) \\ &= \sum r_i \varphi(P_i(T_{P_i})) \\ &= \sum r_i P_i(\varphi(T_{P_i})) \\ &= \sum r_i P_i(a_{P_i}) \\ &= \sum r_i 0 \\ &= 0 \neq 1\end{aligned}$$

□

Now, by 3.2, there exists a max ideal $I \subset \mathcal{M} \subset R$. Put $L = R/\mathcal{M}$. By 2.8, L is a field. For every $P \in S$, let $a_P \in L$ be the image of T_P . Then $P(a_P) = 0$. □

Proof. of Theorem 12.4. We apply the above Lemma (12.5) inductively to obtain

$$K = K_0 \subset K_1 \subset \dots$$

Put $L = \bigcup_{n \geq 0} K_n$. Then L is a field. To see that L is algebraically closed, let $P \in L[T] \setminus L$. Write $P(T) = a_n T^n \dots a_0$. There exists N such that $a_n \dots a_0 \in K_N$. Thus, $P \in K_N[T]$. By construction, we have that there is $a_P \in K_{N+1}$ such that $P(a_P) = 0$. □

13. FEBRUARY 3, 2017

Definition 13.1. 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 13.2. 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 12.1, $\bar{K}(a)$ is algebraic over k , hence a is algebraic over k . Thus $a \in \bar{K}$. □

Corollary 13.3. Every field has an algebraic closure.

Proof. 12.4 and 13.2. □

Proposition 13.4. 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 (3.5) 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 by 6.1, $T^{p^m} - 1$ has at most p^m distinct roots. Oops! This contradicts $|G| = p^n$. □

Finite Fields

Fact 13.5. 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 $\mathbb{Z} \rightarrow F$ (1.7) cannot be injective. Hence the characteristic of F is $p > 0$. 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. □

Proposition 13.6. *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 (13.3). Consider the map $\sigma : \bar{\mathbb{F}}_p \rightarrow \bar{\mathbb{F}}_p$ defined by $x \mapsto x^{p^n}$. 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 $|F| = p^n$. \square

Proposition 13.7. *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 11.1. On the other hand, $|F_1^\times| = p^n - 1 \rightarrow a^{p^n} = a$ 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 13.4 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 13.8. *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 13.6 and 13.7, F_1 is isomorphic to $\mathbb{F}_{p^{\sigma_1}}$ and F_2 is isomorphic to $\mathbb{F}_{p^{\sigma_2}}$, 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_1 and hence $|F_2|$ is a power of $|F_1|$ and so $k|n$.*

14. FEBRUARY 6, 2017

Remark. For L, K fields, if we want to make L into an extension of K , we need to specify a morphism $K \rightarrow L$. (Note that any such morphism is injective, since it is a morphism of fields.) If there is such a morphism, there is usually more than one. **Galois theory** studies these morphisms.

Definition 14.1. Let L/K be an extension, $P \in K[T] \setminus K$. L is a **minimal splitting field of P** provided that i) P splits into linear factors over L , and ii) L is generated by the zeroes of P (i.e. $L = K(a_1, \dots, a_n)$ where $\{a \in L : P(a) = 0\} = \{a_1, \dots, a_n\}$).

Definition 14.2. Let $L_1/K, L_2/K$ be field extensions. A **morphism of extensions** $L_1 \rightarrow L_2$ is a morphism of K -algebras between field extensions of K . The set of all such morphisms is notated $\text{Mor}_K(L_1, L_2)$.

Remark. If K is a field, $(L_1, \varphi_1), (L_2, \varphi_2)$ are extensions, and $f : L_1 \rightarrow L_2$ is a morphism of extensions, i.e.

$$\begin{array}{ccc} L_1 & \xrightarrow{f} & L_2 \\ & \swarrow \varphi_1 & \searrow \varphi_2 \\ & K & \end{array}$$

then we say that f extends φ_2 .

Definition 14.3. An extension L/K is **primitive** provided that $L = K(a)$ for some $a \in L$.

Proposition 14.4. *Let $K(a)/K$ be a primitive extension, M/K be an arbitrary extension. Then*

$$\begin{aligned} \text{Mor}_K(K(a), M) &\rightarrow \{x \in M : M_{a/K}(x) = 0\} \\ \varphi &\mapsto \varphi(a) \end{aligned}$$

is a bijection.

Proof. To show the map is well-defined, i.e. maps into the intended target, consider $\varphi \in \text{Mor}_K(K(a), M)$. Then $M_{a/K}(\varphi(a)) = \varphi(M_{a/K}(a)) = \varphi(0) = 0$, as desired.

To show injectivity, let $\phi, \psi \in \text{Mor}_K(K(a), M)$ s.t. $\phi(a) = \psi(a)$. Let $\rho: K \rightarrow M$ be the morphism defining M as a K -extension. Then for each $y \in K(a)$ we have $y = k_n a^n + \cdots + k_1 a + k_0$ for $k_i \in K$ (if this is not obvious, one might peruse 11.1). Then

$$\begin{aligned} \phi(y) &= \phi(k_n a^n + \cdots + k_1 a + k_0) \\ &= \sum_{i=0}^n \phi(k_i) \phi(a) \\ &= \sum_{i=0}^n \rho(k_i) \phi(a) \\ &= \sum_{i=0}^n \rho(k_i) \psi(a) \\ &= \sum_{i=0}^n \psi(k_i) \psi(a) \\ &= \psi(y), \end{aligned}$$

by the commutativity of the natural extension diagram (see Remark 1.2 above), so we conclude $\phi \equiv \psi$.

To show surjectivity, let $x \in M$ be s.t. $M_{a/K}(x) = 0$. Consider the evaluation morphism $\phi_x: K[T] \rightarrow M$ defined by $T \mapsto x$. (see 5.1) Then $M_{a/K} \in \ker(\phi_x)$, so by the homomorphism theorem (2.3) ϕ_x factors through the quotient $K[T]/(M_{a/K})$, i.e. $\phi_x = K[T] \xrightarrow{\pi} K[T]/(M_{a/K}) \xrightarrow{:(} M$, however we have that $K(a) \simeq K[T]/(M_{a/K})$ by 11.1, so we have the following diagram

$$\begin{array}{ccc} K[T] & \xrightarrow{\phi_x} & M \\ & \searrow \pi & \nearrow :(\\ K(a) & \xrightarrow{:(} & K[T]/(M_{a/K}) \end{array}$$

where $:($ is an isomorphism. Letting $F = :(\circ \pi$ we have $F(a) = x \in M$ as desired. We conclude that the given map is indeed a bijection. \square

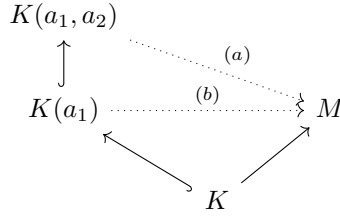
Corollary 14.5. *Let L/K be a finite extension generated by $a_1, \dots, a_n \in L$. Let M/K be an extension s.t. each minimal polynomial $M_{a_1/K}, \dots, M_{a_n/K}$ admits a root in M . Then $\text{Mor}_K(L, M) \neq \emptyset$.*

Proof. We consider the restriction maps

$$\text{Mor}_K(K(a_1, \dots, a_n), M) \xrightarrow{\text{Res}} \text{Mor}_K(K(a_1, \dots, a_{n-1}), M) \xrightarrow{\text{Res}} \cdots \xrightarrow{\text{Res}} \text{Mor}_K(K, M).$$

Each restriction map is surjective, so there composition is as well. Then since $\text{Mor}_K(K, M) \ni (K \hookrightarrow M)$, i.e. the map defining M as a K -extension, then we have $\text{Mor}_K(K(a_1, \dots, a_n), M) \neq \emptyset$ as desired. \square

Remark. To understand what's going on here, consider the $n = 2$ case. We have the following diagram:



The dashed arrow marked (a) represents all morphisms that make the outer diagram commute; the set of all these morphisms is $\text{Mor}_K(K(a_1, a_2), M)$. It restricts to the set of all morphisms making the inner diagram commute, represented by the dashed arrow marked (b); this set is $\text{Mor}_K(K(a_1), M)$. The restriction map functions as follows.

$$\begin{aligned} \text{Mor}_K(K(a_1, a_2), M) &\xrightarrow{\text{Res}} \text{Mor}_K(K(a_1), M) \\ \text{Mor}_{K(a_1)}(K(a_1, a_2), M) &\mapsto \phi. \end{aligned}$$

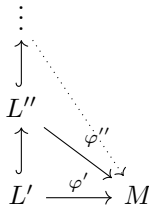
That is: think of ϕ in the role of (b) in the diagram. Then anything that maps to ϕ under Res is a map in the role of (a) that makes the outer diagram commute, but in order to restrict to ϕ , the upper triangle must commute as well. The set of all such maps, those that make the outer and upper diagrams commute, is $\text{Mor}_{K(a_1)}(K(a_1, a_2), M) \subset \text{Mor}_K(K(a_1, a_2), M)$. Since $K(a_1, a_2)$ is a primitive extension of $K(a_1)$, we apply 14.4 above to get the result that $\text{Mor}_{K(a_1)}(K(a_1, a_2), M) \neq \emptyset$. This process is repeated arbitrarily many times in the proof of 14.5. The following corollary proves a similar result for arbitrary (non-primitive) chains of algebraic extensions.

Corollary 14.6. *Let L/K be an algebraic extension and let M/K be an algebraically closed extension. Then $\text{Mor}_K(L, M) \neq \emptyset$.*

Proof. Define the set \mathcal{M} of pairs (L', φ') where $L/L'/K$ and $\varphi' \in \text{Mor}_K(L', M)$. Introduce a partial order on \mathcal{M} by

$$(L', \varphi') \leq (L'', \varphi'') \Leftrightarrow L' \subset L'', \quad \varphi''|_{L'} = \varphi'.$$

Then let $C \subset \mathcal{M}$ be a chain (i.e. a totally ordered subset). C comprises the following diagram



Then taking the union of all such $L \in C$, we get an upper bound for C . $\mathcal{M} \neq \emptyset$ since letting $\mathcal{M} = K$ and φ be the identity gives an element. Then by Zorn's lemma there exists a maximal element $(L_m, \varphi_m) \in \mathcal{M}$. We want to show that this is in fact L . If not, let $a \in L \setminus L_m$. Then φ_m makes M into an L_m -algebra, and since M is algebraically closed, M_{a/L_m} admits a zero in M . By 14.4, $\text{Mor}_{L_m}(L_m(a), L_m) \neq \emptyset$. Taking $\varphi^{\text{contr}} \in \text{Mor}_{L_m}(L_m(a), L_m)$, the existence of $(L_m(a), \varphi^{\text{contr}})$ contradicts the maximality of L_m , closing the proof. \square

15. FEBRUARY 8, 2017

Proposition 15.1. *Let L_1, L_2 be two minimal splitting fields of $P \in K[T] \setminus K$. Then $L_1/K \cong L_2/K$*

Proof. We note that both L_2 and L_1 are K -algebras. By (Cor 5, Feb 6 (FIXME)), there exist K -algebra morphisms $\varphi_2 : L_2 \rightarrow L_1$ and $\varphi_1 : L_1 \rightarrow L_2$.

$$\begin{array}{ccc} L_1 & \overset{\varphi_1}{\dashrightarrow} & L_2 \\ & \nwarrow \quad \nearrow & \\ & K & \end{array}$$

We know that both of these spaces are finite dimensional (so $\dim_K(L_1) < \infty$ and $\dim_K(L_2) < \infty$). These maps are K -linear, and are also morphism of fields, and thus they are injective. Since the dimensions are finite and we have injective maps in both directions, we have that φ_1 and φ_2 are in fact isomorphisms. \square

Proposition 15.2. *Let L/K be a finite extension. The following are equivalent.*

- (1) L is the minimal splitting field of some $P \in K[T] \setminus K$.
- (2) For every $a \in L$, $M_{a/K}$ decomposes into linear factors in $L[T]$.
- (3) For any extension M/K , all K -algebra morphisms $L \rightarrow M$ have the same image.

Definition 15.3. A finite extension L/K is called **normal** if it satisfies the conditions above.

Example. $K = \mathbb{Q}$, $L = \mathbb{Q}[T]/(T^2 + 1)$.

Checking the conditions: If we consider $M = \mathbb{C}$, $a \in L$ defined as the image of T (that is, the coset $T + (T^2 + 1)$) we know that the set of K algebra morphisms from $K(a)$ (which is isomorphic to L) we have a bijection between morphisms and roots of $T^2 + 1 \in \mathbb{C}$. namely i and $-i$. So, the two morphisms are defined by sending $a \rightarrow i$ and $a \rightarrow -i$. Both of these morphisms have image exactly $\mathbb{Q}[i]$.

Example. A nonexample: $K = \mathbb{Q}$, $L = \mathbb{Q}[T]/(T^3 - 2)$.

Again by logic above, we have three morphisms defined for all the roots of $T^3 - 2$ in \mathbb{C} , which are $\sqrt[3]{2}$ multiplied by the 3rd roots of unity. However, we note that the morphism that sends $a \mapsto \sqrt[3]{2}$ has image $\{a + \sqrt[3]{2}b \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$

However, the others, as they have complex parts in their roots of unity, do not map into \mathbb{R} . Thus, the images do not agree.

Some intuition: $\mathbb{Q}[T]/(T^3 - 2)$ adds a single root but not all three needed to split. This, in contrast with $\mathbb{Q}(\zeta_3)[T]/(T^3 - 2)$ (where ζ_3 is a non real third root of unity) only needs to add $\sqrt[3]{2}$ to split.

16. FEBRUARY 10, 2017

Proof. (of 15.2) We prove the loop $1 \Rightarrow 3 \Rightarrow 2 \Rightarrow 1$.

$1 \Rightarrow 3$) It's enough to show this for algebraically closed M . For if we've shown the result for \overline{M} , the restriction $\text{im}(\text{Mor}_K(L, \overline{M}))$ to M gives the result for general M .

Now take L/K the minimal splitting field for P , i.e. finite and satisfying $L = K(a_1, \dots, a_k)$ for $a_i \in L$ the zeroes of P . Then we have $P(T) = (T - a_1)^{m_1} \cdots (T - a_k)^{m_k}$. Now take $f \in \text{Mor}_K(L, M)$ for M/K an algebraically closed extension. Then

$$\prod_{i=1}^k (T - a_i)^{m_i} = P(T) \stackrel{(1)}{=} f(P)(T) = \prod_{i=1}^k (T - f(a_i))^{m_i}$$

where (1) is true since f fixes each $k \in K$, so in particular it fixes $P \in K[T]$. Then we have that $M \supset \{f(a_i) : a_i \text{ a zero for } P\} = \{a_i : \text{zeroes of } P\}$, so M contains the zeroes of P .

Then $f(L)$ is a subfield of M generated by the $f(a_i)$, but these are the zeroes of P in M , which are independent of f . Then each $f \in \text{Mor}_K(L, M)$ are generated by the same elements, i.e. have the same image.

3 \Rightarrow 2) Let $a \in L$ and choose an algebraic closure \bar{L} of L (exists by 13.3). Then let $a = a_1, \dots, a_k \in \bar{L}$ be the zeroes of M_a/K in \bar{L} . By 14.4 we have a one-to-one correspondence $\text{Mor}_K(K(a), \bar{L}) \leftrightarrow \{\text{zeroes of } M_a/K \text{ in } \bar{L}\}$. Then we may choose $\psi_i: K(a) \rightarrow M$ s.t. $\psi_i(a) = a_i$. Then as per 14.5, choose an extension $\tilde{\psi}_i: L \rightarrow \bar{L}$ of ψ_i . Then $\tilde{\psi}_i \in \text{Mor}_K(L, \bar{L})$ with $a \mapsto a_i$. Then by assumption, the inclusion map $L \hookrightarrow \bar{L}$ has the same image as $\tilde{\psi}_i$, so $a_i \in L$.

2 \Rightarrow 1) Write $L = K(a_1, \dots, a_n)$ for some $a_1, \dots, a_n \in L$. Then letting $P = \prod_{i=1}^n M_{a_i/K} \in K[T]$, we have that L is the minimal splitting field of a polynomial $P \in K[T]$. \square

Fact 16.1. *Let L/K be a finite extension. Then there exists a finite extension N/L s.t. N/K is normal.*

Proof. Write $L = K(a_1, \dots, a_n)$ and put $P = \prod M_{a_i/K}$. The splitting field N of P is as needed. N is the **normal closure** of L/K . \square

Fact 16.2. *If $M/L/K$ is a tower of finite extensions with M normal over K , then M is normal over L .*

Proof. If $P \in K[T]$ is the polynomial such that M is the splitting field of K , we have $P \in L[T]$. \square

Proposition 16.3. *Let $L/K, M/K$ be extensions with L/K finite. Then*

$$|\text{Mor}_K(L, M)| \leq [L : K].$$

Proof. We have $L = K(a_1, \dots, a_n)$ for some $a_1, \dots, a_n \in L$. We induct on n .

For $n = 1$, by 14.4, we have

$$\begin{aligned} |\text{Mor}_K(L, M)| &= |\{x \in M : M_{a/K}(x) = 0\}| \\ &\leq \deg(M_{a/K}) \quad \text{by 6.1,} \\ &= [L : K] \quad \text{by 11.1.} \end{aligned}$$

For induction, consider $K(a_1, \dots, a_n)/K(a_1, \dots, a_{n-1})/K$. Then

$$\begin{aligned} \text{Mor}_K(K(a_1, \dots, a_n), M) &\xrightarrow{\text{Res}} \text{Mor}_K(K(a_1, \dots, a_{n-1}), M) \\ \text{Mor}_{K(a_1, \dots, a_{n-1})}(K(a_1, \dots, a_n), M) &\mapsto \{\varphi\}. \end{aligned}$$

Then

$$\begin{aligned} |\text{Mor}_{K(a_1, \dots, a_{n-1})}(K(a_1, \dots, a_n), M)| &\leq [K(a_1, \dots, a_n) : K(a_1, \dots, a_{n-1})] \text{ by base case} \\ |\text{Mor}_K(K(a_1, \dots, a_{n-1}), M)| &\leq [K(a_1, \dots, a_{n-1}), K] \quad \text{by hypothesis,} \\ \Rightarrow [K(a_1, \dots, a_n), M] &\leq [K(a_1, \dots, a_n) : K(a_1, \dots, a_{n-1})] \cdot [K(a_1, \dots, a_{n-1}) : K] \text{ by 10.8,} \\ &= [K(a_1, \dots, a_n) : K] \\ &= [L : K] \end{aligned}$$

with $[K(a_1, \dots, a_n), M] = |\text{Mor}_K(K(a_1, \dots, a_n), M)|$. This completes the proof. \square

Remark. If we have equality in the base case, it descends through the inductive case. When is this true? The answer to this question motivates the following:

Definition 16.4. Let L/K be a finite extension. An element $a \in L$ is called **separable over K** provided that all zeroes of $M_{a/K}$ in its splitting field are simple, i.e. have order 1.

Fact 16.5. *Let $M/L/K$ be a finite tower. If $a \in M$ is separable over K , then it is separable over L .*

Proof. This is a quick exercise in definitions. We have $M_{a/L} \mid M_{a/K}$, so if $M_{a/K}$ splits simply in its splitting field, so must $M_{a/L}$ in the splitting field reduced to the field generated by its zeroes. Thus a is separable over L . \square

17. FEBRUARY 13, 2017

Proposition 17.1. *Let L/K be a finite extension. Then the following are equivalent:*

- every $a \in L$ is separable over K ;
- $L = K(a_1, \dots, a_n)$ for $a_i \in L$ separable over K ;
- if M/L is an extension s.t. M/K is normal, then $|\text{Mor}_K(L, M)| = [L : K]$.

Proof. $1 \Rightarrow 2$) This is trivial.

$2 \Rightarrow 3$) Apply the same argument as in Prop. 3, Feb 10 16.3, replacing “ \leq ” with “ $=$ ”. We can do this since $|\{x \in M : M_{a/K}(x) = 0\}| = \deg(M_{a/K})$, where the desired roots exist since M/K is normal and they are distinct since a is separable.

$3 \Rightarrow 1$) We prove the contrapositive: if $a \in L$ is not separable over K , then $|\text{Mor}_K(L/M)| < [K(a) : K]$, then induct. \square

Definition 17.2. A finite extension is called **separable** provided that it satisfies these conditions.

Corollary 17.3. *Let L/K be a finite extension. The set of all $a \in L$ separable over K is a subfield of L .*

Proof. Let $S \subset L$ be the above set, and $M := K(S) \subset L$ be the subfield generated by S . Now $[M : K] \leq [L : K] < \infty$ so there exist $a_1, \dots, a_n \in S$ such that $M = K(a_1, \dots, a_n)$. Then by Proposition 1 17.1 M is separable, so $M \subset S$. Thus $M = S$. \square

Definition 17.4. M is called the **separable closure of K in L** . $[M : K]$ is the **separability degree**, notated $[L : K]_{\text{sep}}$; $[L : M]$ is the **inseparability degree**, notated $[L : K]_{\text{insep}}$.

Proposition 17.5. (*Primitive Element Theorem*) *Let L/K be a finite separable extension. Then there exists $a \in L$ s.t. $L = K(a)$.*

Proof.

Lemma 17.6. *Let F be an infinite field, V be a finite-dimensional F -vector space, $W_1, \dots, W_n \subset V$ proper subspaces. Then $V \neq \bigcup W_i$.*

of Lemma. This was proved on MATH 494 Problem Set 6. \square

If K is finite, so is L , so L^\times is cyclic (13.4). Then any generator $a \in L^\times$ works. If K is infinite, let \bar{L} be an algebraic closure of L . Then let $\varphi_1, \dots, \varphi_n : L \rightarrow \bar{L}$ be the elements of $\text{Mor}_K(L, \bar{L})$, so $n = [L : K]$. For any $1 \leq i \neq j \leq n$ $\varphi_i - \varphi_j$ is a nonzero morphism of K -vector spaces. Let $W_{i,j} \subsetneq L$ be its kernel. By Lemma 1.6, $L \neq \bigcup W_{i,j}$, so let $a \in L \setminus (\bigcup W_{i,j})$, so $\varphi_i(a) \neq \varphi_j(a)$ for all $1 \leq i \neq j \leq n$. Then $\varphi_1|_{K(a)}, \dots, \varphi_n|_{K(a)}$ are distinct elements of $\text{Mor}_K(K(a), \bar{L})$, so $[L : K] = n \leq [K(a) : K] \leq [L : K]$ since $K(a) \subset L$ (see 16.3). Then $K(a) = L$. \square

Remark. Let L/K be a finite extension. Then every element of $\text{Mor}_K(L, L)$ is invertible, and we can compose them. So $\text{Mor}_K(L, L)$ is a group.

Definition 17.7. $\text{Mor}_K(L, L) =: \text{Aut}(L/K) =: \text{Aut}_K(L)$.

Definition 17.8. A finite extension L/K is called **Galois** provided that $|\text{Aut}(L/K)| = [L : K]$. In that case we write $\text{Gal}(L/K) := \text{Aut}(L/K)$ is its **Galois group**.

18. FEBRUARY 15, 2017

Example.

- \mathbb{C}/\mathbb{R} is Galois, $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \tau\}$, where $\tau(z) = \bar{z}$.
- E/F a quadratic extension, $\text{char}(F) \neq 2$, is Galois. $\text{Gal}(E/F) = \{1, \tau\}$, $\tau(a) = -a$.
This comes from the fact that in Homework, we showed that if $[E : F]$ is 2, we have the existence of $\alpha \in E \setminus F$ such that $\alpha^2 \in F$. We have that $T^2 - a^2 \in F[T]$ is the minimal polynomial, and we know the roots of the minimal polynomial are in bijection with the morphisms from E to E in this case. Thus, the automorphisms are solely determined by how they act on a and $-a$, hence the above 2 morphisms.
- $\mathbb{F}_{q^m}/\mathbb{F}_q$ is Galois with $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \cong \mathbb{Z}/m\mathbb{Z}$ and is generated by $\text{Frob}_q(x) = x^q$.
- (Non-Example): $L = \mathbb{F}_p(T)$, $K = \mathbb{F}_p(T^p) \subset L$. We note that $L = K(T)$ (adjoining T). For $P(x) = X^p - T^p \in K[X]$, we have that T is a root. Thus, the minimal polynomial of T in K divides $X^p - T^p$, so we have $[L : K] \mid p$. As p is prime, we have this index is 1 or p , but as $L \neq K$, it cannot be 1. Thus, $[L : K] = p$. Moreover, this implies L is the splitting field of P , because $L[T], P(X) = (X - T)^p$.
Now, we characterize automorphisms. Take $\varphi \in \text{Aut}(L/K)$. Then, we have $\varphi(T)^p = \varphi(T^p)$. Because $T^p \in K$ and φ fixes K , we have that this equals T^p . Thus, $0 = \varphi(T)^p - T^p = (\varphi(T) - T)^p$. Thus, $\varphi(T) = T$, meaning, as every automorphism fixes both the base field and the element we adjoin, we have $\text{Aut}(L/K) = \{1\}$.

Recall, for G a group, X a set.An **action** of G on X is a group homomorphism from $G \rightarrow \text{Bij}(X)$. The action is called

- **transitive** if $\forall x, y \in X, \exists g \in G$ such that $gx = y$.
- **faithful** if $\forall x \in X, gx = x \Rightarrow g = 1$.
- **simple** if $\exists x \in X, gx = x \Rightarrow g = 1$.

Some notation:

- $G \cdot x = \{g \cdot x \mid g \in G\} \subset X$ is the **orbit** of x .
- $G_x = \{g \in G \mid gx = x\} \subset G$ is the **stabilizer** of x .
- $X^G = \{x \in X \mid gx = x \forall g \in G\}$

 $G/G_x \cong G \cdot x$ by the map $g \mapsto g \cdot x$ (orbit-stabilizer)If $y = gx$, then $Gg = gG_xg^{-1}$.If this action is transitive and all stabilizers have the same size, the action is **simply transitive** and $|G| = |X|$.**Definition 18.0.** If L is a field, $\text{Aut}(L)$ is the group of field automorphisms of L .*Remark.* If L/K is an extension, the $\text{Aut}(L/K) = \{\sigma \in \text{Aut}(L) \mid \sigma(k) = k \forall k \in K\}$. That is, the map restricts to the identity on K .If $G \subset \text{Aut}(L)$, then L^G is a subfield of L . Each $\sigma \in \text{Aut}(L)$ acts on $L[T]$ by $\sigma(a_n T^n + \dots a_0) = \sigma(a_n) T^n + \dots \sigma(a_0)$. By 5.1 we have $L \xrightarrow{\sigma} L \hookrightarrow L[T]$ that sends $T \mapsto T$. If we have $K = L^G$, then $L[T]^G = K[T]$.**Proposition 18.1.** Let L/K be a finite extension. The following are equivalent.

- (1) L/K is Galois
- (2) L/K is normal and separable
- (3) $K = L^{\text{Aut}(L/K)}$

(4) For every $a \in L$, $M_{a/K}(T) = \prod_{\eta \in G \cdot a} (T - \eta)$ where $G = \text{Aut}(L/K)$

Proof. 2) \Rightarrow 1) Immediate from 17.1.

1) \Rightarrow 3) $|G| = [L : K] \geq [L : L^G] \geq |G|$ as $G \subset \text{Mor}_{L^G}(L, L)$ and by 16.3. This string of inequalities thus implies that $[L : K] = [L : L^G]$ which implies that $K = L^G$.

3) \Rightarrow 4) Let $Q(T) = \prod_{\eta \in G \cdot a} (T - \eta) \in L[T]$. Now we note that $Q(a) = 0$. Now, $\forall \sigma \in G$, we have that $\sigma(Q)$

simply permutes the ordering on the orbit, and thus $\sigma(Q) = Q$. This means that $Q \in K[T]$, as $K[T]$ is by assumption the field fixed by $\text{Aut}(L/K)$. Now, we also note that every $b \in G \cdot a$ is a zero of $M_{a/K}$, because $b = \sigma(a)$ for $\sigma \in G$, and is thus a zero of $\sigma(M_{a/K})$. However, σ also fixes $M_{a/K}$, which means b is a zero of $M_{a/K}$. Now, this implies thus that $Q \mid M_{a/K}$ in $L[T]$. Since we know that both are now in $K[T]$, we also thus have that $Q \mid M_{a/K}$ in $K[T]$. However, by 11.1, $M_{a/K}$ is irreducible, so we have $M_{a/K} = Q$, as desired.

4) \Rightarrow 2) By 4) $M_{a/K}$ splits completely over L with distinct roots, so L/K is normal and separable. \square

19. FEBRUARY 17, 2017

Recall: E/F finite extension is Galois. Then

$$|\text{Aut}(E/F)| = [E : F] \iff$$

it's normal and separable \iff

$$E^{\text{Aut}(E/F)} = F \iff$$

$$M_{a/F}(T) = \prod_{b \in G \cdot a} (T - b) = Q, Q \mid M_{a/F}, M_{a/F} \text{ is irreducible}$$

by 11.1. Every $b \in G \cdot a$ is a zero of $M_{a/F} : b = \sigma(a), \sigma \in G$ is a zero of $\sigma(M_{a/F}) = M_{a/F}$. We call $\mathbb{F}_p(T) = K, \mathbb{F}_p(T^p) = L$. We have that $M_{T/K}(X) = X^p - T^p$, $M_{T/K} \mid X^p - T^p \rightarrow M_{T/K}$ is a repeated root and is irreducible (PS4P11) which implies that $p \mid \deg(M_{T/K})$ which implies that $M_{T/K} = X^p - T^p$.

Proposition 19.1. Let E be a field, $G \in \text{Aut}(E)$ a finite subgroup. Put $F = E^G$. Then E/F is a finite Galois extension with group G .

Proof.

Claim. Any $a \in E$ is algebraic and separable over F , $\deg(a/F) \leq |G|$, and E contains all zero's of $M_{a/F}$.

Proof. $Q(T) = \prod_{b \in G \cdot a} (T - b)$. Again, $\sigma Q = Q$ for all $\sigma \in G$, so $Q \in F[T]$. Moreover, $Q(a) = 0$. Thus a is algebraic over F , $\deg(a/F) \leq \deg(Q) \leq |G|$. Moreover $M_{a/F} \mid Q$ and thus has distinct zeros, so a is separable over F and all zero's of $M_{a/F}$ are also zeros of Q , hence in E . \square

Claim. Let $E/M/F$ with M/F finite. Then M/F is separable, $[M : F] \leq |G|$, and E contains the normal closure of M .

Proof. Claim 1 implies that M/F is separable and E contains the normal closure of M . By 17.5, $M = F(a)$ for some $a \in M$. Then $[M, F] = \deg(a/F) \leq |G|$ (by claim 1). \square

Claim. E/F is finite.

Proof. By claim 1, E/F is algebraic. If $[E : F] = \infty$, here is a tower $F \subset M_1 \subset M_2 \subset \dots$ of finite extensions contained in E such that $[M_i : F] \rightarrow \infty$. This contradicts claim 2. \square

Now E/F is a finite, hence separable and normal by claim 2, hence Galois. From $G \subset \text{Gal}(E/F)$ we get $|G| \leq |\text{Gal}(E/F)| = [E : F] \leq |G|$ by claim 2. \square

Theorem 19.2. Let E/F be a finite Galois extension with $G = \text{Gal}(E/F)$. We let

$$A = \{E/M/F \text{ intermediate fields}\}, B = \{H \subset G \text{ subgroups}\}$$

and the maps

$$M \in A \longrightarrow \text{Gal}(E/M) \in B, H \in B \longrightarrow E^H \in A$$

are (i) mutually inverse, inclusion reversing, G -equivariant bijections.

(ii) Given $M \iff H$ TFAE. (a) M/F is normal, (b) M is a G invariant, (c) $H \subset G$ is a normal subgroup. In that case, the restriction map $G \longrightarrow \text{Gal}(M/F)$ induces an isomorphism $G/H \cong \text{Gal}(M/F)$.

(iii) Given $E/M, L/F$, $\text{Gal}(E/M/L) = \text{Gal}(E/M) \cap \text{Gal}(E/L)$.

Proof. (i) Since E/F is normal and separable so is E/M by 16.2 and PS6P2. Thus E/M is Galois. Setting $H = \text{Gal}(E/M)$, then $E^H = M$ by 18.1. Conversely, starting $H \subset G$ subgroup, and let $M = E^H$, hence E/M is Galois by 18.1 (with Galois group H). Moreover $F \subset M$, since $H \subset G$.

(ii) (b) \iff (c) immediate from equivariance. (a) \iff (b) follows from the fact that G acts transitively on the zeros of $M_{a/F}$, for each $a \in E$ M is normal, have M is the splitting field of some P , hence generated over F by its 0's. But G permutes them, so leaves M invariant. If M is G -invariant, $a \in M$, then since G permutes the zeros of $M_{a/F}$ transitively, all of them belong to M . Now consider $G \longrightarrow \text{Gal}(M/F)$. By definition, its kernel is $\text{Gal}(E/M)$. So get injective morphism $G/H \longrightarrow \text{Gal}(M/F)$. Both sides have size $[E:F]/[E:M] = [M:F]$.

(iii) Immediate (supposedly). □

20. FEBRUARY 20, 2017

Recall: E/F finite, Galois with group $\text{Gal}(E/F)$.

$$\begin{aligned} E/M/F &\xleftrightarrow{1-1} H \leq G \\ M &\longmapsto \text{Gal}(E/M) = \{\sigma \in \text{Gal}(E/F) : \sigma|_M = \text{id}_M\} \\ E^H &\hookrightarrow H \end{aligned}$$

and: M/F normal $\Leftrightarrow M$ G -invariant $\Leftrightarrow H \trianglelefteq G \longrightarrow G/H \xrightarrow{\text{Res}} \text{Gal}(M/F)$.

Proposition 20.1. Let L/K be an extension, $L/E, F/K$ such that $E/K, F/K$ are finite. If E/K is Galois, EF/F is Galois and

$$\text{Gal}(EF/F) \xrightarrow{\text{Res}|_E} \text{Gal}(E/E \cap F).$$

is an isomorphism.

Proof. By assumption there is $P \in K[T]$ with simple roots s.t. E is the splitting field of P . Write $E = K(a_1, \dots, a_m)$ for a_i in some algebraic closure of K , with $P(a_i) = 0$ for each $i \leq m$. Then if $F = K(b_1, \dots, b_\ell)$, then $EF = \{\sum_{i=1}^m e_i \cdot f_i : m \in \mathbb{N}, f_i \in F, e_i \in E\} = F(a_1, \dots, a_m)$. Then we can see that EF is the splitting field of P over F . In particular, EF/F is Galois.

Now let $\sigma \in \text{Gal}(EF/F)$; σ permutes the zeroes of P and fixes K , so it fixes E set-wise. Since (by definition) it fixes F point-wise, the restriction $\sigma \xrightarrow{\text{Res}|_E} \sigma|_E$ is well-defined (with $\sigma|_E \in \text{Gal}(E/E \cap F)^3$). To show that $\text{Res}|_E$ is injective, suppose that σ is in the kernel of the restriction map. Then it fixes E and F , thus EF as well, so σ is the identity. To show it is surjective, take $H \leq \text{Gal}(E/E \cap F)$ be the image of

³ $E/E \cap F$ is Galois by 16.2 and Problem 2, Problem Set 6.

$\text{Res}|_E$. Its fixed field is $E \cap F$, so $\text{Gal}(E/E \cap F)$ and H have the same fixed field. By Galois correspondence (19.2) they are equal. \square

Proposition 20.2. (*Independence of characters*) Let G be a finite group, K be a field, and $\psi_1, \dots, \psi_n : G \rightarrow K^\times$ be distinct homomorphisms. Then in the K -vector space $\text{Maps}(G, K)$ ψ_1, \dots, ψ_n are linearly independent.

Proof. Suppose they aren't. Then after reordering assume that ψ_1, \dots, ψ_k are minimally linearly independent, i.e. any proper subset of them is linearly independent. Then there exist $a_1, \dots, a_k \in K$ not all zero so that

$$a_1\psi_1(g) + a_2\psi_2(g) + \dots + a_k\psi_k(g) = 0 \quad (*)$$

for all $g \in G$. Choose $z \in G$ s.t. $\psi_1(z) \neq \psi_2(z)$. Then

$$a_1\psi_1(zg) + a_2\psi_2(zg) + \dots + a_k\psi_k(zg) = 0.$$

This is

$$\begin{aligned} a_1\psi_1(z)\psi_1(g) + a_2\psi_2(z)\psi_1(g) + \dots + a_k\psi_k(z)\psi_k(g) &= 0 \\ a_1\psi_1(g) + a_2\frac{\psi_2(z)}{\psi_1(z)}\psi_2(g) + \dots + a_k\frac{\psi_k(z)}{\psi_1(z)}\psi_k(g) &= 0. \quad (**) \end{aligned}$$

Then taking the difference $(*) - (**) we have a linear relation between ψ_2, \dots, ψ_k which is nontrivial since the coefficient in front of ψ_2 is $\left(1 - \frac{\psi_2(z)}{\psi_1(z)}\right) \neq 0$. This contradiction closes the proof. $\square$$

Remark. The above proof holds if G is a monoid, i.e. does not contain all of its inverses.

Corollary 20.3. Let L/K be finite. Then elements of $\text{Aut}(L/K)$ are linearly independent in the K -vector space $\text{End}_K(L)$.

Proof. Apply Proposition 2 (20.2) to restrictions of $\sigma \in \text{Aut}(L/K)$ to L^\times , which are group homomorphisms $L^\times \rightarrow L^\times$. \square

Lemma 20.4. Let L/K be a finite Galois extension with group $G = \{\sigma_1, \dots, \sigma_n\}$. Given $e_1, \dots, e_n \in L$ the following are equivalent:

- 1) e_1, \dots, e_n is a basis for the K -vector space L ;
- 2) $[\sigma_1(e_1) \ \dots \ \sigma_n(e_1)]^{tr}, \dots, [\sigma_1(e_n) \ \dots \ \sigma_n(e_n)]^{tr}$ is a basis for the L -vector space L^n .

Proof. Consider the matrix

$$A = \begin{bmatrix} \sigma_1(e_1) & \dots & \sigma_1(e_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(e_1) & \dots & \sigma_n(e_n) \end{bmatrix}$$

The following are equivalent:

- A invertible;
- the columns of A are linearly independent;
- the rows of A are linearly independent.

Then: 1) \Rightarrow 2): Consider a linear relation between the rows, $\lambda_1, \dots, \lambda_n \in L$ such that

$$\begin{aligned} \lambda_1\sigma_1(e_1) + \dots + \lambda_n\sigma_n(e_1) &= 0 \\ \lambda_1\sigma_1(e_2) + \dots + \lambda_n\sigma_n(e_2) &= 0 \\ &\vdots \end{aligned}$$

Then $\sum \lambda_i \sigma_i \in \text{End}_K(L)$ vanishes on the basis e_1, \dots, e_n , so $\sum \lambda_i \sigma_i \equiv 0$. Then by Cor. 3 above (20.3) $\lambda_1 = \dots = \lambda_n = 0$.

2) \Rightarrow 1): Take $\lambda_1, \dots, \lambda_n \in L$ so that $\sum \lambda_i e_i \equiv 0$. Apply $\sigma_1, \dots, \sigma_n$ to this relation to get

$$\begin{aligned}\lambda_1 \sigma_1(e_1) + \dots + \lambda_n \sigma_1(e_n) &= 0 \\ \lambda_1 \sigma_2(e_1) + \dots + \lambda_n \sigma_2(e_n) &= 0 \\ &\vdots \\ \lambda_1 \sigma_n(e_1) + \dots + \lambda_n \sigma_n(e_n) &= 0.\end{aligned}$$

This is

$$\begin{aligned}A \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix} &= \vec{0} \\ \Rightarrow \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix} &= A^{-1} \vec{0} = \vec{0}.\end{aligned}$$

□

21. FEBRUARY 22, 2017

Theorem 21.1. *Let L/K be a finite Galois extension, $\text{Gal}(L/K) = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$. There exists $a \in L$ such that $\{\sigma_1(a), \sigma_2(a), \dots, \sigma_n(a)\}$ is a basis of the K -vector space L .*

Remark. The G -representation L is isomorphic to the regular representation $K[G]$.

Proof. We consider 2 cases on the size of K .

Case 1: K is infinite. By 20.4, we are looking for $a \in L$ such that

$$A = (\sigma_i^{-1} \sigma_j(a))_{i,j} \text{ is invertible}$$

i.e. $\det(A) \neq 0$. Choose a basis e_1, \dots, e_n of the K -vector space L . Thus, any $a \in L$ is of the form $a_1 e_1 + \dots + a_n e_n$ with $a_i \in K$. Thus, we have that

$$A = \left(\sum_{k=1}^n a_k \sigma_i^{-1} \sigma_j(e_k) \right)_{i,j}$$

Define $p(a_1, \dots, a_n) = \det(A)$ for the above A . Then, $p \in L[T_1, \dots, T_n]$. We claim that $p \neq 0$.

Proof. (of claim.) By 20.4, there exist $c_1, \dots, c_n \in L$ such that

$$c_1 \begin{bmatrix} \sigma_1(e_1) \\ \vdots \\ \sigma_n(e_1) \end{bmatrix} + \dots + c_n \begin{bmatrix} \sigma_1(e_n) \\ \vdots \\ \sigma_n(e_n) \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \end{bmatrix}$$

Which means that

$$\sum_{k=1}^n c_k \sigma_i^{-1} \sigma_j(e_k) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

This gives us the associated matrix A for the c coefficients is the identity, meaning that $p(c_1, \dots, c_n) = \det(I_n) = 1$. As we have values for which p is nonzero, we have that $p \neq 0$, as desired. □

Now, since K is infinite, we can find values $a_1 \dots a_n \in K$ where $p(a_1, \dots, a_n)$ is nonzero. This implies the associated determinant is nonzero, so we have values that give us the desired matrix being invertible, as desired. Thus, we have $a_1 e_1 + \dots a_n e_n$ being the value $a \in L$ that we are looking for.

Case 2: K is finite. Then, $\text{Gal} = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ where $\sigma = \text{Frob}_q$ and $q = |K|$. These are all distinct, hence linearly independent over L by 20.3 hence over K .

Thus, the minimal polynomial of $\sigma \in \text{End}_{K\text{-vs}}(L)$ has degree n (it can't be $< n$ as $1, \sigma, \dots, \sigma^{n-1}$ are linearly independent, and it is $\leq n$ as the characteristic polynomial is degree n). Thus, the minimal polynomial is the characteristic polynomial.

Thus, the K -vector space L has a cyclic vector. \square

Cyclotomic Extensions of \mathbb{Q}

Definition 21.2. $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$

We define a homomorphism

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\times &\longrightarrow \text{Aut}(\mu_n) \\ a &\longmapsto (z \mapsto z^a) \end{aligned}$$

Fact 21.3. *The map defined above is an isomorphism.*

Proof. If $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $z^{ab} = (z^a)^b$

Injective $z^a = z^b \Leftrightarrow z^{a-b} = 1 \Leftrightarrow a - b \equiv 0(n) \Leftrightarrow a \equiv b(n)$.

Surjective Let $\varphi \in \text{Aut}(\mu_n)$, and $\zeta = e^{\frac{2\pi i}{n}} \in \mu_n$. Then, $\varphi(\zeta) = \zeta^a$. Moreover, since $\varphi^{-1}(\zeta) = \zeta^b$ for some other b , we have $\zeta = \varphi^{-1}(\varphi(\zeta)) = \zeta^{ab}$. Thus $ab - 1 \equiv 0(n)$, meaning $ab \equiv 1(n)$, so $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. \square

22. FEBRUARY 24, 2017

We let $M_n = \{z \in \mathbb{C}^\times \mid z^n = 1\}$ and

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \text{Aut}(M_n)$$

defined by

$$a \longrightarrow (z \longmapsto z^a).$$

Fact 22.1. *The following are equivalent: (1) $\{d \in \mathbb{N} \mid 1 \leq d \leq n, (d, n) = 1\}$ (2) $|\{\text{generators of } \mathbb{Z}/n\mathbb{Z}\}|$ (3) $|(\mathbb{Z}/n\mathbb{Z})^\times|$*

Proof. $\text{ord}(d, \mathbb{Z}/n\mathbb{Z}) = \text{lcm}(d, n)/d$,

$$\text{ord}(d, \mathbb{Z}/n\mathbb{Z}) = n \iff \text{lcm}(d, n) = nd \iff \gcd(d, n) = 1$$

$$(1) \iff (3) \quad d \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \exists e = d^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$$

$$n|ed - 1 \iff \exists k \in \mathbb{Z} : ed = 1 + nk$$

Then $d \in (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow d$ and n have no common divisors if and only if $(d, n) = 1$. If $(d, n) = 1 \longrightarrow \exists a, b \in \mathbb{Z} : ad + bn = 1 \iff ad \equiv 1 \pmod{n}$. \square

$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, the Euler ϕ function.

Fact 22.2. (i) If n, m are coprime, then $\phi(n, m) = \phi(n)\phi(m)$. (ii) If p is prime, $\phi(p^r) = p^{r-1}(p-1)$. (iii) $\sum_{d|n} \phi(d) = n$.

Proof. (i) By the Chinese Remainder Theorem (3.5), we have isomorphisms

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

of rings, hence also an isomorphism of unit groups

$$(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times.$$

(ii) $a \in \mathbb{Z}$ is not coprime to p^r if and only if $p|a$. There are exactly p^{r-1} -many multiplies of p between 1 and p^r . Thus $\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$. (iii) Let $d|n$. Then $\mathbb{Z}/d\mathbb{Z}$ injects into $\mathbb{Z}/n\mathbb{Z}$ defined by $x \mapsto n/d \cdot x$ with image $\{y \in \mathbb{Z}/n\mathbb{Z} | dy = 0\}$. Thus $\phi(d) = |\{y \in \mathbb{Z}/n\mathbb{Z} | \text{ord}(y) = d\}|$. \square

Recall: $\Phi_n(T) = \prod_{S \in M_n, \text{ord}(S)=n} (T - S) \in \mathbb{Z}[T] \subset \mathbb{C}[T]$.

Proposition 22.3. Φ_n is irreducible in $\mathbb{Q}[T]$.

Proof. Assume not. Write $\Phi_n = f \cdot g$ (non-constant), $f \cdot g \in \mathbb{C}[T]$. After rescaling we may assume $f \in \mathbb{Z}[T]$ is primitive. Then $g \in \mathbb{Z}[T]$, see 8.4.

Claim. If $f(S) = 0$ and p does not divide n is prime, then $f(S^p) = 0$.

Proof. Assume not. Then from $\Phi_n(S^p) = 0$ we get that $g(S^p) = 0$. Thus S is a 0 of $g(T^p)$. Then f and $G(T^p)$ have a non-trivial gcd in $\mathbb{C}[T]$, hence by PS4P9 also in $\mathbb{Q}[T]$. Since f is irreducible, we have $f|g(T^p)$. Since f is primitive, get $f|g(T^p)$ in $\mathbb{Z}[T]$ by 8.4. Let \bar{f}, \bar{g} be the images of f, g in $\mathbb{F}_p[T]$. Then $\bar{f}|\bar{g}(T^p)$. But $\bar{g}(T^p) = \bar{g}^p$. So $\bar{f}|\bar{g}^p$. Thus \bar{f} and \bar{g} have a common divisor. Thus \bar{f} and \bar{g} have a common zero in \mathbb{F}_p so $\bar{\Phi}_n$ has a multiple zero in \mathbb{F}_p , which is impossible by PS4P10. So $x^n - 1$ will have a multiple 0 in \mathbb{F}_p . \square

Admitting this, choose any $S \in M_n, f(S) = 0$. For any other $S' \in M_n, \text{ord}(S') = n$. There is $a \in \mathbb{Z}, (a, n) = 1, S' = S^a$. Apply claim to prime decomposition of a to conclude $f(S') = 0$. Thus $f = \Phi_n$. \square

Definition 22.4. The n^{th} cyclotomic extension of \mathbb{Q} is $\mathbb{Q}(M_n)$.

Proposition 22.5. The map $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Gal}(Q(M_n)/Q), a \mapsto (z \mapsto z^a)$ is an isomorphism. In particular, $[Q(M_n) : Q] = \phi(n)$.

Proof. Enough, by 22.2, to show that the restriction map $\text{Gal}(Q(M_n)/Q) \rightarrow \text{Aut}(M_n)$ defined by $\sigma \mapsto \sigma|_{M_n} (M_n \subset \mathbb{C}/M_n)^\times$ preserves M_n , so this map is well-defined. Let $S \in M_n$ have order n . Then $Q(M_n) = Q(S)$ by 14.4, and $M_{S/a} = \Phi_n$ by 22.3. So,

$$\text{Gal}(Q(S)/Q) \cong \{z \in Q(S) | \Phi_n(S) = 0\} = \{z \in M_n | \text{ord}(z) = n\}.$$

\square