

RINGS AND FIELDS

ALIREZA SALEHI GOLSEFIDY

CONTENTS

1. Lecture 1: Zeros of polynomials and algebra, recalling cyclic groups and basic properties of order of elements.	1
2. Lecture 2: statements needed from group theory, definition of ring, unital, commutative, units, zero-divisors, ring homomorphism.	6
3. Lecture 3: characteristic of a ring, Chinese Remainder Theorem, Euler's ϕ function, fields.	10
4. Lecture 4: computing Euler ϕ -function, integral domains, cancellation law, characteristic of an integral domain, connections between fields and integral domains, definition of fractions.	13
5. Lecture 5: the universal property of field of fractions	16
6. Lecture 6: how to use the universal property of field of fractions, defining degree, leading term and coefficient of polynomials, division algorithm, nilpotent elements and their connection with units.	18
7. Lecture 7: division algorithm, factor theorem, generalized factor theorem, number of distinct zeros over an integral domain.	21
8. Lecture 8: zeros of polynomials in direct products, Fermat's little theorem, Frobenius homomorphism, factorization of $x^p - x$ over $\mathbb{Z}_p$, Wilson's theorem, irreducible elements, irreducible polynomials over a field, having zero and factorization, degree 2 or 3 irreducibility criterion.	24
9. Lecture 9: rational root criterion and its applications. no zero mod p implies no rational zero. content of a polynomial and its basic properties.	28
10. Lecture 10: Gauss's lemma, versions 1,2, and 3. Mod- p irreducibility criterion. Eisenstein's irreducibility criterion.	32
11. Lecture 11: ideal, ideals generated by a given set of elements, principal ideals, kernels are ideals, ideals of a field, PID.	36
12. Lecture 12: quotient ring, fundamental theorem of homomorphism, evaluation map revisited, algebraic elements	37
13. Lecture 13: Minimal polynomial, correspondence theorem, maximal ideals, irreducible elements in a PID and maximal ideals.	40
14. Lecture 14: Maximal ideals of PIDs and irreducible elements. Image of the evaluation map at an algebraic element. Prime ideals. Prime elements. Connection between prime and irreducible	43

1. LECTURE 1: ZEROS OF POLYNOMIALS AND ALGEBRA, RECALLING CYCLIC GROUPS AND BASIC PROPERTIES OF ORDER OF ELEMENTS.

Most of algebra has been developed to study the zeros of polynomials, beginning with degree one and two polynomials in a single variable. Throughout this course, we will keep this motivation

in mind and view the abstract concepts we introduce through the lens of their connections to polynomials.

1.1. Recalling some concepts from group theory. We briefly recall some concepts from group theory. You must review these concepts thoroughly.

Definition 1. A group G is a non-empty set together with two operations:

$$G \times G \rightarrow G, \quad (x, y) \mapsto x \cdot y \quad \text{and} \quad G \rightarrow G, \quad x \mapsto x^{-1},$$

that satisfy the following properties:

- (1) (Associative) $\forall x, y, z \in G, \quad (x \cdot y) \cdot z = x \cdot (y \cdot z).$
- (2) (Neutral element) There exists $e_G \in G$ such that for all $x \in G, e_G \cdot x = x \cdot e_G = x.$
- (3) (Inverse) For all $x \in G, x \cdot x^{-1} = x^{-1} \cdot x = e_G.$

Suppose $(G, \cdot)$ is a group. For every $g \in G$ and $n \in \mathbb{Z}^+$, we let

$$g^n := \underbrace{g \cdot \dots \cdot g}_{n\text{-times}}.$$

Define $g^0 := e_G$ and $g^{-n} := (g^n)^{-1}.$

Recall that, for all $a \in G,$

$$a \cdot a^{-1} = a^{-1} \cdot a = e_G \quad \text{implies that} \quad (a^{-1})^{-1} = a.$$

For all $a, b \in G,$

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e_G \cdot a^{-1} = a \cdot a^{-1} = e_G,$$

and similarly,

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot e_G \cdot b = b^{-1} \cdot b = e_G.$$

Hence, for all $a, b \in G,$

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}.$$

In particular, for all positive integer $n,$

$$(1) \quad a^{-n} = (a^n)^{-1} = \underbrace{(a \cdot \dots \cdot a)^{-1}}_{n\text{-times}} = \underbrace{(a^{-1} \cdot \dots \cdot a^{-1})}_{n\text{-times}} = (a^{-1})^n.$$

Lemma 1. Suppose $(G, \cdot)$ is a group. For every $a \in G$ and $m, n \in \mathbb{Z},$

$$a^m \cdot a^n = a^{m+n} \quad \text{and} \quad (a^m)^n = a^{mn}.$$

Proof. Suppose m, n are positive integers. Then

$$a^m \cdot a^n = \underbrace{a \cdot \dots \cdot a}_{m\text{-times}} \cdot \underbrace{a \cdot \dots \cdot a}_{n\text{-times}} = \underbrace{a \cdot \dots \cdot a}_{m+n\text{-times}} = a^{m+n},$$

and

$$(a^m)^n = \underbrace{(a \cdot \dots \cdot a)^n}_{m\text{-times}} = \underbrace{((\underbrace{a \cdot \dots \cdot a}_{m\text{-times}}) \cdot \dots \cdot (\underbrace{a \cdot \dots \cdot a}_{m\text{-times}}))}_{n\text{-times}} = \underbrace{(a \cdot \dots \cdot a)}_{mn\text{-times}} = a^{mn}.$$

Suppose $m = 0.$ Then

$$a^0 \cdot a^n = e_G \cdot a^n = a^n = a^{0+n}$$

and

$$(a^0)^n = e_G^n = e_G.$$

Suppose $n = 0.$ Then

$$a^m \cdot a^0 = a^m \cdot e_G = a^m = a^{m+0},$$

and

$$(a^m)^0 = e_G = a^0 = a^{m \cdot 0}.$$

Therefore, so far, we have proved the claims for pairs of non-negative integers.

Suppose $m > 0 > n \geq -m$. So, $n = -n'$ and $m \geq n' > 0$. Then, $a^{m-n'} \cdot a^{n'} = a^m$ as n' and $m - n'$ are non-negative integers. Thus

$$a^m \cdot a^n = (a^{m-n'} \cdot a^{n'}) \cdot (a^{n'})^{-1} = a^{m-n'} \cdot (a^{n'} \cdot (a^{n'})^{-1}) = a^{m-n'} = a^{m+n}.$$

We also have

$$(a^m)^n = ((a^m)^{n'})^{-1} = (a^{mn'})^{-1} = a^{-mn'} = a^{mn}.$$

(Here we do not use the assumption that $n' \leq m$.)

Suppose $m > 0$ and $-m > n$. So, $n = -n'$ and $n' > m$. Therefore, $b^m \cdot b^{n'-m} = b^{n'}$ for all $b \in G$. In particular, we obtain the same equality for $b = a^{-1}$. Thus

$$(a^{-1})^m \cdot (a^{-1})^{n'-m} = (a^{-1})^{n'}.$$

Hence, by (1), we deduce

$$a^{-m} \cdot a^{m-n'} = a^n.$$

It follows that

$$a^m \cdot a^n = a^m \cdot (a^{-m} \cdot a^{m-n'}) = (a^m \cdot a^{-m}) \cdot a^{m-n'} = a^{m+n}.$$

The remaining cases are similar, and we leave them as an exercise. $\square$

The cyclic subgroup of G generated by $g \in G$ is defined to be the smallest subgroup of G which contains g and it is denoted by $\langle g \rangle$.

Lemma 2. $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Proof. Since $g \in \langle g \rangle$ and $\langle g \rangle$ is a subgroup, for every positive integer n ,

$$g^n = \underbrace{g \cdots g}_{n\text{-times}} \in \langle g \rangle.$$

Since $g^n \in \langle g \rangle$ and $\langle g \rangle$ is a subgroup,

$$g^{-n} = (g^n)^{-1} \in \langle g \rangle,$$

for all positive integer n . Since $\langle g \rangle$ is a subgroup, $e_G = g^0 \in \langle g \rangle$. Altogether,

$$\langle g \rangle \supseteq \{g^n \mid n \in \mathbb{Z}\}.$$

By Lemma 1, $\{g^n \mid n \in \mathbb{Z}\}$ is closed under multiplication and taking inverse. Hence, it is a subgroup. We also have that

$$g = g^1 \in \{g^n \mid n \in \mathbb{Z}\}.$$

Therefore, $\{g^n \mid n \in \mathbb{Z}\} \subseteq \langle g \rangle$. This completes the proof. $\square$

Order of an element $g \in G$ is defined to be $|\langle g \rangle|$. It is denoted by $\text{ord}(g)$ or $o(g)$ or $|g|$. The next theorem which is proved in your group theory course gives us the main properties $\text{ord}(g)$.

Theorem 3. Suppose $g \in G$ is of finite order. Then the following statements hold.

- (1) $\text{ord}(g) = d \Leftrightarrow g^n = e_G$ precisely when $d \mid n$. Moreover, $\langle g \rangle = \{e_G, g, \dots, g^{\text{ord}(g)-1}\}$.
- (2) For $n_1, n_2 \in \mathbb{Z}$, $g^{n_1} = g^{n_2}$ if and only if $n_1 \equiv n_2 \pmod{\text{ord}(g)}$.

Proof. Since $\langle g \rangle$ is finite, there exists $m < m'$ such that $g^m = g^{m'}$. Therefore, $g^{m'-m} = e_G$ and $m' - m$ is a positive integer. Hence, by the well-ordering principle, there exists the smallest positive integer d_0 with the property that $g^{d_0} = e_G$.

Claim 1. $g^n = e_G$ if and only if $d_0 \mid n$.

Proof of Claim 1. ($\Leftarrow$) Since $d_0|n$, for some integer k , $n = d_0k$. Hence, by Lemma 1,

$$g^n = g^{d_0k} = (g^{d_0})^k = e_G^k = e_G.$$

($\Rightarrow$) By the division algorithm, there exists a unique pair (q, r) of integers such that $n = d_0q + r$ and $0 \leq r < d_0$ – recall that q is called the quotient of n divided by d_0 and r is called the remainder of n divided by d_0 . Thus,

$$g^n = e_G \quad \text{implies} \quad g^{d_0q+r} = e_G.$$

Therefore

$$e_G = g^{d_0q} \cdot g^r = (g^{d_0})^q \cdot g^r = e_G^q \cdot g^r = g^r.$$

Since $r < d_0$, d_0 is the smallest positive integer with the property that $g^{d_0} = e_G$, and $g^r = e_G$, we deduce that r is not positive. On the other hand, since r is a remainder, it is non-negative. Therefore, $r = 0$, which implies that $n = d_0q$ is a multiple of d_0 . $\square$

Claim 2 $\langle g \rangle = \{e_G, g, \dots, g^{d_0-1}\}$ and for $0 \leq i < j < d_0$, $g^i \neq g^j$. In particular, $\text{ord}(g) = d_0$.

Proof of Claim 2. Clearly $\{e_G, g, \dots, g^{d_0-1}\} \subseteq \langle g \rangle$. For every $n \in \mathbb{Z}$, by the division algorithm, there exists a unique pair (q, r) of integers such that $n = qd_0 + r$ and $0 \leq r < d_0$. Hence,

$$g^n = g^{qd_0} \cdot g^r = g^r \in \{e_G, g, \dots, g^{d_0-1}\}.$$

Therefore, by Lemma 2,

$$\langle g \rangle \subseteq \{e_G, g, \dots, g^{d_0-1}\}.$$

Altogether, it follows that

$$(2) \quad \langle g \rangle = \{e_G, g, \dots, g^{d_0-1}\}.$$

To show the second part, we proceed by the contradiction. Suppose to the contrary that there exist $0 \leq i < j < d_0$ such that $g^i = g^j$. Then

$$g^{j-i} = e_G, \quad \text{and} \quad 0 < j - i \leq j < d_0,$$

which contradicts the assumption that d_0 is the smallest positive integer with the property that $g^{d_0} = e_G$. The second part implies that

$$|\{e_G, g, \dots, g^{d_0-1}\}| = d_0.$$

Therefore, by (2), we deduce

$$\text{ord}(g) = |\langle g \rangle| = |\{e_G, g, \dots, g^{d_0-1}\}| = d_0.$$

$\square$

Part (1) follows from Claims 1 and 2.

Part (2) ($\Rightarrow$) $g^{n_1} = g^{n_2}$ implies that $g^{n_1-n_2} = e_G$. Then, by Part (1), $\text{ord}(g)|n_1 - n_2$, which implies that

$$n_1 \equiv n_2 \pmod{\text{ord}(g)}.$$

($\Leftarrow$) $n_1 \equiv n_2 \pmod{\text{ord}(g)}$ implies that $\text{ord}(g)|n_1 - n_2$. Hence, by Part (1), $g^{n_1-n_2} = e_G$. Thus, $g^{n_1} = g^{n_2}$. This completes the proof. $\square$

Let's recall the basic properties of congruence arithmetic. We say x is *congruent to* x' *modulo* n and write

$$x \equiv x' \pmod{n} \quad \text{if} \quad \exists k \in \mathbb{Z}, x - x' = nk.$$

We sometimes write $x \stackrel{n}{\equiv} x'$ instead of $x \equiv x' \pmod{n}$. This defines an *equivalence* relation on the set of integers. It means

- (1) (Reflexive) $a \stackrel{n}{\equiv} a$ for all a .
- (2) (Symmetric) $a \stackrel{n}{\equiv} b$ implies $b \stackrel{n}{\equiv} a$.

(3) (Transitive) $a \stackrel{n}{\equiv} b$ and $b \stackrel{n}{\equiv} c$ imply $a \stackrel{n}{\equiv} c$.

Equivalence relations are crucial in various parts of mathematics, e.g. cosets of a subgroup in group theory, identifying two functions that differ on a *measure zero* set in analysis, defining new spaces by *gluing* two subsets in topology, etc. The residue class of a modulo n is denoted by $[a]_n$ and it is defined as

$$[a]_n := \{b \in \mathbb{Z} \mid b \stackrel{n}{\equiv} a\}.$$

Note that $[a]_n$ is an arithmetic progression $a + n\mathbb{Z}$ consisting of a -shifts of multiples of n . Hence,

$$(3) \quad [a]_n = [a']_n \quad \text{if and only if} \quad a \stackrel{n}{\equiv} a'.$$

The following lemma allows us to do congruence arithmetic.

Lemma 4. *If $x \stackrel{n}{\equiv} x'$ and $y \stackrel{n}{\equiv} y'$, then*

$$x + y \stackrel{n}{\equiv} x' + y' \quad \text{and} \quad xy \stackrel{n}{\equiv} x'y'.$$

Proof. You have seen this statement before. I recall the proof of the second part as the same idea will be used later when we define the quotient of a ring by an ideal.

Since $x \stackrel{n}{\equiv} x'$ and $y \stackrel{n}{\equiv} y'$, there exist $k, \ell \in \mathbb{Z}$ such that

$$x - x' = nk \quad \text{and} \quad y - y' = n\ell.$$

Note that

$$xy - x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y') = nky + x'n\ell = n(ky + x'\ell).$$

Hence, $xy \stackrel{n}{\equiv} x'y'$. □

Lemma 4 implies that the following are well-defined operations.

Lemma 5. $[x]_n + [y]_n := [x + y]_n$ and $[x]_n [y]_n := [xy]_n$ are well-defined operations on $\mathbb{Z}_n$.

Whenever representatives are used to define a function on equivalence classes, one must check that the function is well-defined. In colloquial language, we may say that *one has to check that different representatives have the same opinion on the given issue!*

Proof. We must show that $[x]_n = [x']_n$ and $[y]_n = [y']_n$ implies $[x + y]_n = [x' + y']_n$ and $[xy]_n = [x'y']_n$. By (3), we deduce that $x \stackrel{n}{\equiv} x'$ and $y \stackrel{n}{\equiv} y'$. Therefore, by Lemma 4, $x + y \stackrel{n}{\equiv} x' + y'$ and $xy \stackrel{n}{\equiv} x'y'$. Thus, by (3), it follows that $[x + y]_n = [x' + y']_n$ and $[xy]_n = [x'y']_n$. This completes the proof. □

Lemma 6. $(\mathbb{Z}_n, +)$ is a cyclic group.

Proof. Since the addition is defined based on the addition of representatives of residue classes, it is clear that $+$ is associative, $[0]_n$ is the neutral element, and $[-x]_n$ is the additive inverse of $[x]_n$. Note that the cyclic subgroup generated by $[1]_n$ is $\mathbb{Z}_n$. This completes the proof. □

An important concept you learned in group theory is that of a group *homomorphism*. Whenever you study a mathematical structure (or category), you must also study the maps that preserve that structure. Consider the following examples:

- (1) Linear algebra: vector spaces and linear maps.
- (2) Topology: topological spaces and continuous maps.
- (3) Group theory: groups and group homomorphisms.

Recall that $f: G \rightarrow H$ is called a *group homomorphism* if G and H are groups and for all $x, y \in G$,

$$f(xy) = f(x)f(y).$$

A bijective group homomorphism is called a *group isomorphism*.

Theorem 7. Suppose G is a cyclic group of order n . Then $G \simeq \mathbb{Z}_n$.

Proof. Suppose $G = \langle g \rangle$. Let $f: \mathbb{Z}_n \rightarrow G$, $f([a]_n) = g^a$. Since we are using a residue representative to define f , we must show why it is well-defined.

Suppose $[a]_n = [a']_n$. Then $a \equiv a' \pmod{n}$. Since $\text{ord}(g) = n$, by Theorem 3, $g^a = g^{a'}$, which means $f([a]_n) = f([a']_n)$. Therefore, f is well-defined.

Next, we check that f is a group homomorphism. For every $[a]_n, [b]_n \in \mathbb{Z}_n$,

$$f([a]_n)f([b]_n) = g^a g^b = g^{a+b} = f([a+b]_n).$$

Finally, we must show that f is bijective. Since $|G| = n = |\mathbb{Z}_n|$, it is sufficient to prove that f is injective. Suppose $f([a]_n) = f([b]_n)$. Then $g^a = g^b$, so by Theorem 3,

$$a \equiv b \pmod{n} \quad \text{which implies} \quad [a]_n = [b]_n.$$

This completes the proof. $\square$

2. LECTURE 2: STATEMENTS NEEDED FROM GROUP THEORY, DEFINITION OF RING, UNITAL, COMMUTATIVE, UNITS, ZERO-DIVISORS, RING HOMOMORPHISM.

In the previous lecture, we recalled basic properties of order of elements and cyclic groups. You must review the following topics from group theory:

- (1) Cosets of a subgroup, index of a subgroup, and Lagrange's theorem.
- (2) Quotient of a group by a normal subgroup.
- (3) Kernel of a group homomorphism and the fundamental theorem of group homomorphisms, also known as the first isomorphism theorem.

When we are working with an additive group $(A, +)$, instead using the convention of g^n , we write ng . So, for $g \in A$ and $n \in \mathbb{Z}$,

$$ng = \begin{cases} \underbrace{g + \cdots + g}_{n\text{-times}} & \text{if } n > 0. \\ 0 & \text{if } n = 0. \\ -n'g & \text{if } n = -n' \text{ and } n' > 0. \end{cases}$$

By Lemma 1, we deduce that for $g \in A$ and $m, n \in \mathbb{Z}$,

$$mg + ng = (m + n)g \quad \text{and} \quad m(ng) = (mn)g.$$

Quick reminder of the mentioned concepts from group theory: if H is a subgroup of G , then a left coset of H is of the form $gH := \{gh \mid h \in H\}$. The set of all the left cosets

$$G/H := \{gH \mid g \in G\}$$

is a partition of G , and so, we deduce the Lagrange theorem:

$$|G| = |H|[G : H],$$

where $[G : H]$ is called the index of H in G and it is the number of elements of G/H .

A subgroup N of G is called a normal subgroup if for every $g \in G$, $gNg^{-1} = N$. When N is a normal subgroup of G , then $xN \cdot yN := (xy)N$ defines a group structure on G/N . The group G/N is called the quotient of G by N .

For a group homomorphism $f: G \rightarrow H$, the kernel of f is

$$\ker(f) := \{g \in G \mid f(g) = e_H\}.$$

Kernel of f is a normal subgroup of G . The image of f is

$$\text{Im}(f) := \{f(g) \mid g \in G\}.$$

The image of f is a subgroup of H . The fundamental theorem of group homomorphisms states that

$$\bar{f}: G/\ker(f) \rightarrow \text{Im}(f), \quad \bar{f}(g \ker(f)) := f(g)$$

is a well-defined group isomorphism.

Definition 2. A ring R is a set together with two binary operations:

$$R \times R \rightarrow R, (x, y) \mapsto x + y \quad \text{and} \quad R \times R \rightarrow R, (x, y) \mapsto x \cdot y$$

that satisfy the following properties:

- (1) (Additive group) $(R, +)$ is an abelian group.
- (2) (Associative) For all $x, y, z \in R$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- (3) (Distributive) For all $x, y, z \in R$, $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

We say R is commutative if $x \cdot y = y \cdot x$ for all $x, y \in R$. We say R is unital if there exists $1 \in R$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in R$.

Let us see a few examples.

- (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are unital commutative rings.
- (2) $\mathbb{Z}^{\geq 0}$ is not a ring as $(\mathbb{Z}^{\geq 0}, +)$ is not a group.
- (3) $n\mathbb{Z}$ is a commutative ring, but it is not unital.
- (4) $M_2(\mathbb{Z})$ is a unital ring, but it is not commutative.
- (5) $\mathbb{Z}_n$ is a unital commutative ring.

We may construct new rings using old ones:

- (1) (Direct product) Suppose $R_1, \dots, R_n$ are rings. Then componentwise addition and multiplication makes $R_1 \times \dots \times R_n$ into a ring.
- (2) (Direct product) We may have an infinite family of rings and take their product: given $\{R_i\}_{i=1}^{\infty}$, we may consider componentwise addition and multiplication to make $\prod_{i=1}^{\infty} R_i$ into a ring.
- (3) (Matrix ring) For every ring R , the set of n -by- n matrices with entries in R form a ring and it is denoted by $M_n(R)$.
- (4) (Polynomials) For every ring R , let

$$R[x] := \left\{ \sum_{i=0}^n r_i x^i \mid r_i \in R, n \in \mathbb{Z}^{\geq 0} \right\}.$$

We add and multiply polynomials in the usual way.

Lemma 8. Suppose R is a ring. Then the following statements hold.

- (1) For all $a \in R$, $a \cdot 0 = 0 \cdot a = 0$.
- (2) For all $a, b \in R$,

$$(-a) \cdot b = a \cdot (-b) = -(a \cdot b) \quad \text{and} \quad (-a) \cdot (-b) = a \cdot b.$$

Proof. Note that $a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Therefore, $a \cdot 0 = a \cdot 0 + a \cdot 0$. Adding the negative of $a \cdot 0$ to both sides, we deduce that $a \cdot 0 = 0$. Using $(0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$ and a similar argument, we deduce that $0 \cdot a = 0$.

For all $a, b \in R$, we have

$$0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b \quad \text{which implies that} \quad (-a) \cdot b = -(a \cdot b).$$

Using the expression $a \cdot (b + (-b))$ and a similar argument, we obtain that $a \cdot (-b) = -(a \cdot b)$.

Let $a' := -a$. Then $(-a) \cdot (-b) = a' \cdot (-b) = -(a' \cdot b) = -((-a) \cdot b) = -(-(a \cdot b)) = a \cdot b$. This completes the proof. $\square$

Lemma 9. *In a unital ring R , the identity is unique.*

Proof. Suppose 1 and $1'$ are both identities of R . Consider $1 \cdot 1'$. Since 1 is an identity, $1 \cdot 1' = 1'$. As $1'$ is the identity, we deduce that $1 \cdot 1' = 1$. Thus, $1 = 1 \cdot 1' = 1'$. $\square$

Definition 3. Suppose R is a unital ring. An element $r \in R$ is called a unit if it has a multiplicative inverse; that means if there exists $r' \in R$ such that

$$r \cdot r' = r' \cdot r = 1_R.$$

The set of units of R is denoted by $R^\times$.

Let's see a few examples:

- (1) $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.
- (2) $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$.
- (3) $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$. Let's recall that

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} + \left(\frac{-b}{a^2+b^2}\right)i$$

and $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \in \mathbb{R}$ as $a+bi \neq 0$. **The idea of multiplying by conjugates is very useful.**

- (4) $\mathbb{Z}^\times = \{1, -1\}$.

Question. The ring of Gaussian integers is $\mathbb{Z}[i] := \{a+bi \mid a, b \in \mathbb{Z}\}$. You can check that it is closed under subtraction and multiplication, and deduce that it is a subring of $\mathbb{C}$. What is $\mathbb{Z}[i]^\times$?

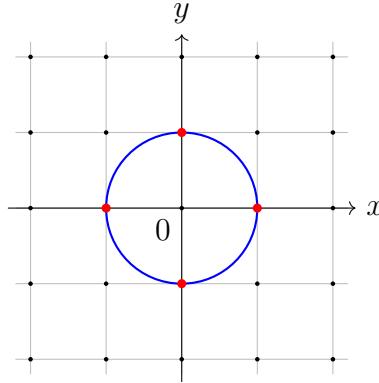
Solution. Suppose for $a, b \in \mathbb{Z}$, $a+bi \in \mathbb{Z}[i]$. Then there exists $r, s \in \mathbb{Z}$ such that

$$(a+bi)(s+ri) = 1.$$

Hence,

$$(4) \quad 1 = |(a+bi)(r+si)|^2 = |a+bi|^2 |r+si|^2 = (a^2+b^2)(r^2+s^2).$$

Since $a, b, r, s \in \mathbb{Z}$, a^2+b^2 and r^2+s^2 are integer numbers. Therefore, by (4), $a^2+b^2 \in \mathbb{Z}^\times$. Since a^2+b^2 is non-negative and it is a unit in $\mathbb{Z}$, we deduce that $a^2+b^2 = 1$.



Hence, $a+bi \in \{1, -1, i, -i\}$. Conversely,

$$1 \cdot 1 = 1, (-1) \cdot (-1) = 1, \text{ and } (i) \cdot (-i) = 1.$$

Hence, $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$. $\square$

Definition 4. A function $f: R \rightarrow S$ is called a ring homomorphism if R and S are rings, and, for all $x, y \in R$,

$$f(x+y) = f(x) + f(y) \quad \text{and} \quad f(x \cdot y) = f(x) \cdot f(y).$$

A bijective ring homomorphism is called a ring isomorphism.

Proposition 10. Suppose R is a unital ring. Then $f: \mathbb{Z} \rightarrow R$, $f(n) := n1_R$ is a ring homomorphism.

We recalled the notation g^n for powers of an element in a group written multiplicatively. For a group $(A, +)$ written additively, we use ng instead of g^n . In this notation, we have:

$$(n + m)g = ng + mg \quad \text{and} \quad n(mg) = (nm)g.$$

It is important to emphasize that ng is **not** multiplication in a ring: the symbols n and g do not belong to the same set.

Proof. For every $n, m \in \mathbb{Z}$,

$$f(n) + f(m) = n1_R + m1_R = (n + m)1_R = f(n + m).$$

Next, we must show that $f(m)f(n) = f(mn)$. We will prove this in a case-by-case argument based on the sign of m and n .

Suppose $m, n > 0$. Then

$$\begin{aligned} f(m)f(n) &= \underbrace{(1_R + \cdots + 1_R)}_{m\text{-times}} \cdot \underbrace{(1_R + \cdots + 1_R)}_{n\text{-times}} \\ &= \underbrace{(1_R \cdot 1_R + \cdots + 1_R \cdot 1_R)}_{mn\text{-times}} \\ &= \underbrace{(1_R + \cdots + 1_R)}_{mn\text{-times}} = (mn)1_R = f(mn). \end{aligned}$$

Suppose $m = 0$. Since $f(0) = 0$, by Lemma 8,

$$0 = f(0) = f(0n) = 0 \cdot f(n) = f(0) \cdot f(n).$$

Similarly, the claim follows if $n = 0$.

Suppose $m > 0 > n$. Set $n' = -n$. Then

$$\begin{aligned} f(m)f(n) &= (m1_R) \cdot (-n'1_R) = -(f(m) \cdot f(n')) \\ &= -f(mn') = -((mn')1_R) = (-mn')1_R = (mn)1_R = f(mn). \end{aligned}$$

(Think about each step and justify them!) □

Problem. Compute $([2]_6x + [1]_6)([3]_6x^2 + x + [1]_6)$ in $\mathbb{Z}_6[x]$.

Solution. We distribute and then add and multiply in the ring $\mathbb{Z}_6$ to find the final answer:

$$\begin{aligned} ([2]_6x + [1]_6)([3]_6x^2 + x + [1]_6) &= [6]_6x^3 + [2]_6x^2 + [2]_6x + [3]_6x^2 + x + [1]_6 \\ &= [5]_6x^2 + [3]_6x + [1]_6. \end{aligned}$$

□

Note that the degree of the first polynomial is 1, and the degree of the second polynomial is 2, but the degree of their product is not the expected $1 + 2$. What is the difference of this case and what you had seen for polynomials over $\mathbb{C}$? Looking at the leading terms, you see that $[2]_6[3]_6 = 0$ though $[2]_6 \neq 0$ and $[3]_6 \neq 0$. Over complex numbers, product of two non-zero elements is always non-zero.

Definition 5. An element $r \in R$ is called a zero-divisor if $r \neq 0$ and $r \cdot r' = 0$ for some non-zero element r' .

So, $\mathbb{C}$ does not have a zero-divisor, but $[2]_6$ and $[3]_6$ are zero-divisors of $\mathbb{Z}_6$.

3. LECTURE 3: CHARACTERISTIC OF A RING, CHINESE REMAINDER THEOREM, EULER'S ϕ FUNCTION, FIELDS.

What can we learn about a ring by focusing just on its additive structure?

Definition 6. The characteristic of a ring R is the smallest positive integer n such that for all $x \in R$, $nx = 0$. If there are no such positive integers, we say R is of characteristic zero.

Note that, by Theorem 3, $nx = 0$ if and only if $\text{ord}(x) | n$. Hence, the characteristic of R satisfies the following property:

$$\text{char}(R) = \begin{cases} \text{lcm}\{\text{ord}(x) \mid x \in R\} & \text{if it is finite,} \\ 0. & \end{cases}$$

When R is a unital ring, it is much easier to compute $\text{char}(R)$.

Proposition 11. Suppose R is a unital ring. Then

$$\text{char}(R) = \begin{cases} \text{ord}(1_R) & \text{if it is finite,} \\ 0. & \end{cases}$$

Proof. If $\text{ord}(1_R) = \infty$, then $\text{char}(R) = 0$, and there is nothing to prove. So, without loss of generality, we may assume that $\text{ord}(1_R) = m < \infty$. For every $a \in R$, we have

$$ma = \underbrace{a + \cdots + a}_{m \text{ times}} = \underbrace{(1_R + \cdots + 1_R)}_{m \text{ times}} \cdot a = (m1_R) \cdot a = 0 \cdot a = 0.$$

Hence, $0 < \text{char}(R) \leq m$. Note that $\text{char}(R)1_R = 0$ implies that $m | \text{char}(R)$. Since $\text{char}(R)$ is positive, we deduce $\text{char}(R) \geq m$. Altogether, it follows that $\text{char}(R) = m$. $\square$

Question. What is the characteristic of $2\mathbb{Z}_4$?

Solution. Note that $2\mathbb{Z}_4$ is not a unital ring and we cannot use Proposition 11 to determine the characteristic of this ring.

Since $2[1]_4 = [2]_4 \neq 0$, the characteristic is not 1. On the other hand, $2(2\mathbb{Z}_4) = 4\mathbb{Z}_4 = 0$. Therefore, the characteristic is 2. $\square$

Exercise 1. Think about the characteristic of $m\mathbb{Z}_n$.

Outline of a solution. From group theory, we know that

$$\text{ord}(g^k) = \frac{\text{ord}(g)}{\gcd(k, \text{ord}(g))}.$$

In the additive form, we obtain

$$\text{ord}_+(kx) = \frac{\text{ord}_+(x)}{\gcd(k, \text{ord}_+(x))}.$$

Using this formula, deduce that

$$\text{ord}_+(m[1]_n) = \frac{n}{\gcd(m, n)}.$$

Also observe that

$$\frac{n}{\gcd(m, n)}(m\mathbb{Z}_n) = \underbrace{\left(\frac{m}{\gcd(m, n)}\right)}_{\text{is an integer}} n\mathbb{Z}_n = 0.$$

Deduce that $\text{char}(m\mathbb{Z}_n) = \frac{n}{\gcd(m, n)}$.

Question. What is the characteristic of $R := \mathbb{Z}_2 \times \mathbb{Z}_3 \times \cdots$?

Solution. Suppose $\text{char}(R) = m$ and $m \neq 0$. Note that for all n , there is a copy of $\mathbb{Z}_n$ in the $n-1$ -th component of R . Hence, knowing that $mx = 0$ for all $x \in R$ implies that $m\mathbb{Z}_n = 0$. This implies that $m \geq n$ for all n . This is a contradiction. Thus, $\text{char}(R) = 0$. $\square$

Question. What is the characteristic of $R := \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$?

Solution. Note that $2R = 0$ and $R \neq 0$. Hence, $\text{char}(R) = 2$. This examples provides us with an infinite ring with finite characteristic. $\square$

Lemma 12. For every $n \geq 2$, $c_n: \mathbb{Z} \rightarrow \mathbb{Z}_n$, $c_n(a) := [a]_n$ is a surjective ring homomorphism and its kernel is $n\mathbb{Z}$.

Recall that the kernel of group homomorphism $f: (A, +) \rightarrow B$ is

$$\ker f := \{a \in A \mid f(a) = 0\}.$$

Proof. For every $a, b \in \mathbb{Z}$,

$$\begin{aligned} c_n(a) + c_n(b) &= [a]_n + [b]_n = [a + b]_n = c_n(a + b) \\ c_n(a) \cdot c_n(b) &= [a]_n \cdot [b]_n = [ab]_n = c_n(ab). \end{aligned}$$

Hence, c_n is a ring homomorphism. Every element of $\mathbb{Z}_n$ is of the form $[a]_n = c_n(a)$. Therefore, c_n is surjective.

Note that $a \in \ker c_n$ if and only if $c_n(a) = 0$. We have

$$c_n(a) = 0 \Leftrightarrow [a]_n = 0 \Leftrightarrow n|a \Leftrightarrow a \in n\mathbb{Z}.$$

Thus, $\ker c_n = n\mathbb{Z}$. $\square$

Question. When is the map $c_{n,m}: \mathbb{Z}_n \rightarrow \mathbb{Z}_m$, $c_{n,m}([a]_n) := [a]_m$ well-defined?

Solution. Let's try the case of $n = 2$ and $m = 3$. Is $c_{2,3}$ well defined? It means assuming two integers a_1 and a_2 have the same *opinion* on the issue of divisibility by 2, do they have the same *opinion* on the issue of divisibility by 3?

If we choose representatives based on one issue, on what other issues are they going to agree on?

Note that $[2]_2 = [0]_2$ but $[2]_3 \neq [0]_3$. So, $c_{2,3}$ is not well defined.

Following the same idea, assuming $c_{n,m}$ is well defined, we deduce

$$[0]_n = [n]_n \text{ implies that } c_{n,m}([0]_n) = c_{n,m}([n]_n) \text{ and so } [0]_m = [n]_m. \text{ Therefore } m|n.$$

Does the converse hold: assuming $m|n$, can we prove that $c_{n,m}$ is well defined? The answer yes. Let's go over the proof. We must show

$$[a_1]_n = [a_2]_n \text{ implies } c_{n,m}([a_1]_n) = c_{n,m}([a_2]_n) \text{ which means } [a_1]_m = [a_2]_m.$$

We start with the assumption and present a direct proof:

$$[a_1]_n = [a_2]_n \Rightarrow a_1 \stackrel{n}{\equiv} a_2 \Rightarrow n|a_1 - a_2.$$

$$\text{Since } m|n \text{ it follows } m|a_1 - a_2 \Rightarrow a_1 \stackrel{m}{\equiv} a_2 \Rightarrow [a_1]_m = [a_2]_m.$$

$\square$

The above answer shows the following lemma:

Lemma 13. $c_{n,m}: \mathbb{Z}_n \rightarrow \mathbb{Z}_m$, $c_{n,m}([x]_n) := [x]_m$ is well-defined if and only if $m|n$.

Lemma 14. Suppose $m|n$. Then $c_{n,m}: \mathbb{Z}_n \rightarrow \mathbb{Z}_m$, $c_{n,m}([a]_n) = [a]_m$ is a well-defined surjective ring homomorphism.

Proof. By Lemma 13, $c_{n,m}$ is well-defined. Next, we show that it is a ring homomorphism. For all $x, y \in \mathbb{Z}$,

$$\begin{aligned} c_{n,m}([x]_n) + c_{n,m}([y]_n) &= [x]_m + [y]_m = [x + y]_m = c_{n,m}([x + y]_n) = c_{n,m}([x]_n + [y]_n), \\ c_{n,m}([x]_n) \cdot c_{n,m}([y]_n) &= [x]_m \cdot [y]_m = [xy]_m = c_{n,m}([xy]_n) = c_{n,m}([x]_n \cdot [y]_n). \end{aligned}$$

Note that every element of $\mathbb{Z}_m$ is of the form $[x]_m = c_{n,m}([x]_n)$ which is in the image of $c_{n,m}$. Hence, $c_{n,m}$ is surjective. $\square$

Theorem 15 (Chinese Remainder Theorem). *Suppose $\gcd(m, n) = 1$. Then*

$$c: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n, \quad c([a]_{mn}) := ([a]_m, [a]_n)$$

is a well-defined isomorphism.

Proof. Note that $c([x]_{mn}) = (c_{mn,m}([x]_{mn}), c_{mn,n}([x]_{mn}))$. Since $m|mn$ and $n|mn$ by Lemma 14, $c_{mn,m}$ and $c_{mn,n}$ are well-defined ring homomorphisms. Therefore, c is a well-defined ring homomorphism. Next, we must show that c is a bijection. Note that

$$|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|,$$

and so it suffices to prove that c is injective. Suppose $c([x]_{mn}) = c([y]_{mn})$. Then

$$\begin{aligned} ([x]_m, [x]_n) &= ([y]_m, [y]_n) \Rightarrow \begin{cases} [x]_m = [y]_m \\ [x]_n = [y]_n \end{cases} \\ &\Rightarrow \begin{cases} x \equiv y \pmod{m} \\ x \equiv y \pmod{n} \end{cases} \\ &\Rightarrow \begin{cases} m|x - y \\ n|x - y \end{cases} \\ &\Rightarrow \text{lcm}(m, n)|x - y. \end{aligned}$$

Since $\gcd(m, n) = 1$, $\text{lcm}(m, n) = mn$. Thus,

$$mn|x - y, \quad \text{which implies that } x \equiv y \pmod{mn} \quad \text{and so } [x]_{mn} = [y]_{mn}.$$

This implies c is injective which completes the proof. $\square$

Theorem 16. $\mathbb{Z}_n^\times = \{[a]_n \mid \gcd(a, n) = 1\}$.

Proof. By definition, $[a]_n \in \mathbb{Z}_n^\times$ if and only if there exists $x \in \mathbb{Z}$ such that $[a]_n[x]_n = [1]_n$. We have

$$\begin{aligned} [a]_n[x]_n = [1]_n &\Leftrightarrow [ax]_n = [1]_n \Leftrightarrow ax \equiv 1 \pmod{n} \\ &\Leftrightarrow \exists y \in \mathbb{Z}, ax - 1 = ny. \end{aligned}$$

Altogether, it follows that

$$(5) \quad [a]_n \in \mathbb{Z}_n^\times \Leftrightarrow \exists x, y \in \mathbb{Z}, ax - ny = 1.$$

In your earlier courses, you have seen the following statement: For every $a, b, c \in \mathbb{Z}$,

$$\exists x, y \in \mathbb{Z}, ax + by = c \Leftrightarrow \gcd(a, b) | c.$$

Therefore, by (5), we deduce

$$[a]_n \in \mathbb{Z}_n^\times \Leftrightarrow \gcd(a, n) = 1.$$

This completes the proof. $\square$

Let $\phi(n) := |\mathbb{Z}_n^\times|$. It is called Euler's ϕ function

Corollary 17. Suppose $\gcd(m, n) = 1$. Then $\mathbb{Z}_{mn}^\times \simeq \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$. In particular,

$$\phi(mn) = \phi(m)\phi(n).$$

Proof. By the CRT, $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$. So, $\mathbb{Z}_{mn}^\times \simeq (\mathbb{Z}_m \times \mathbb{Z}_n)^\times$. By your HW assignment,

$$(\mathbb{Z}_m \times \mathbb{Z}_n)^\times = \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times.$$

This completes the proof of the first part.

Note that

$$\phi(mn) = |\mathbb{Z}_{mn}^\times| = |\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times| = |\mathbb{Z}_m^\times| \cdot |\mathbb{Z}_n^\times| = \phi(m)\phi(n).$$

□

If p is prime, then for every $0 < a < p$, $\gcd(a, p) = 1$. Hence,

$$\mathbb{Z}_p^\times = \{[1]_p, \dots, [p-1]_p\} = \mathbb{Z}_p \setminus \{0\}.$$

This takes us to the definition of a field.

Definition 7. A unital commutative ring F is called a field if $F^\times = F \setminus \{0\}$.

Example 1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}_p$, for a prime p , are fields. $\mathbb{Z}$ is not a field. $\mathbb{Q}[\sqrt{3}]$ is a field as you have seen in your HW assignment.

If $n > 0$ is a composite number, then $n = rs$ for some $r, s \geq 2$. Then

$$\gcd(r, n) = r \neq 1 \quad \text{and} \quad [r]_n \neq 0.$$

Hence, $\mathbb{Z}_n^\times \neq \mathbb{Z}_n \setminus \{0\}$. Therefore, $\mathbb{Z}_n$ is not a field if n is composite. This implies:

Lemma 18. For $n \geq 2$, $\mathbb{Z}_n$ is a field if and only if n is prime.

4. LECTURE 4: COMPUTING EULER ϕ -FUNCTION, INTEGRAL DOMAINS, CANCELLATION LAW, CHARACTERISTIC OF AN INTEGRAL DOMAIN, CONNECTIONS BETWEEN FIELDS AND INTEGRAL DOMAINS, DEFINITION OF FRACTIONS.

Using the CRT, we proved that $\phi(mn) = \phi(m)\phi(n)$ if $\gcd(m, n) = 1$. This helps us reduce the problem of computing $\phi(n)$ to that of powers of primes:

$$\phi(p_1^{k_1} \cdots p_m^{k_m}) = \phi(p_1^{k_1}) \cdots \phi(p_m^{k_m})$$

if p_i 's are distinct primes. Note that

$$\phi(p^k) = |\{[a]_{p^k} \mid \gcd(a, p^k) = 1\}|,$$

and, for a prime number p ,

$$\gcd(a, p^k) = 1 \quad \text{if and only if} \quad p \nmid a.$$

Hence

$$\phi(p^k) = |\{a \mid 1 \leq a \leq p^k\}| - |\{a \mid 1 \leq a \leq p^k, p|a\}| = p^k - p^{k-1}.$$

Problem. Find the number of units of $\mathbb{Z}_{100}$.

Solution. $\phi(100) = \phi(2^2 5^2) = \phi(2^2)\phi(5^2) = (2^2 - 2)(5^2 - 5) = (2)(20) = 40$. □

Let's recall that $a \in R$ is called a zero-divisor if $a \neq 0$ and there exists $b \in R$ such that $ab = 0$ and $b \neq 0$. For instance, $[3]_{15}$ is a zero-divisor of $\mathbb{Z}_{15}$ as $[3]_{15}[5]_{15} = [0]_{15}$ and $[3]_{15}$ and $[5]_{15}$ are non-zero.

Definition 8. A unital commutative ring D is called an integral domain if $0 \neq 1$ and D has no zero-divisors.

Let us remark that if in a unital ring R , $0 = 1$, then $R = \{0\}$. Here is the proof: for all $r \in R$, we have

$$r = 1_R \cdot r = 0_R \cdot r = 0_R.$$

So, the condition $0 \neq 1$ is equivalent to saying that the ring has more than one element. The ring that has only 0 is called the trivial ring.

The major property of integral domains is on having the *cancellation law*. We say a ring R has the cancellation law if for every non-zero $a \in R$,

$$a \cdot b = a \cdot c \quad \text{implies} \quad b = c.$$

Lemma 19. *A unital commutative ring D with $0 \neq 1$ is an integral domain if and only if it satisfies the cancellation law.*

Proof. ($\Rightarrow$) Suppose $a \cdot b = a \cdot c$. Then $a \cdot (b - c) = 0$. Since D does not have a zero-divisor and $a \neq 0$, we deduce that $b - c = 0$. Therefore, $b = c$.

($\Leftarrow$) By assumption, D is a unital commutative ring and $0 \neq 1$. So it suffices to argue why D does not have a zero-divisor. Suppose to the contrary that a is a zero-divisor. Then there exists $b \in D \setminus \{0\}$ such that $a \cdot b = 0$. It follows that $a \cdot b = a \cdot 0$. Since D has the cancellation law and $a \neq 0$, we deduce that $b = 0$ which is a contradiction. $\square$

Lemma 20. *Suppose R is a unital commutative ring. Prove that if $r \in R^\times$, the r is not a zero-divisor.*

Proof. Suppose to the contrary that there exists a unit a which is a zero-divisor. Then there exist $a^{-1} \in R$ and at the same time $b \in R \setminus \{0\}$ such that $a \cdot b = 0$. Multiply both sides of this equation by a^{-1} . Then,

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \quad \text{which implies that} \quad (a^{-1} \cdot a) \cdot b = 0 \quad \text{and so} \quad b = 0.$$

We obtain a contradiction, which completes the proof. $\square$

Corollary 21. *Every field is an integral domain*

Proof. Suppose a is a zero-divisor of F . Then by Lemma 20, we deduce that a is not a unit. This is a contradiction as every non-zero element of a field is a unit. Hence, F has no zero-divisor.

Are we done? No! We must check other conditions: (1) is F unital commutative? (2) Is $0 \neq 1$?

The first one follows from the fact that every field is unital commutative.

The second one follows from $1 \in F^\times = F \setminus \{0\}$. Now, the proof is completed. $\square$

Clearly the converse of Corollary 21 does not hold as $\mathbb{Z}$ is an integral domain which is not field. Next, we show that the converse holds for *finite rings*.

Proposition 22. *A finite ring D is a field if and only if it is an integral domain.*

Proof. ($\Rightarrow$) Follows from Corollary 21. ($\Leftarrow$) Since D is an integral domain, it is a unital commutative ring and $0 \neq 1$. So, in particular, $0 \notin D^\times$ (note that if $0 \in D^\times$, then $0_D \cdot a = 1_D$ for some $a \in D$, which implies that $0_D = 1_D$. This contradicts the assumption that D is an integral domain.) This means $D^\times \subseteq D \setminus \{0\}$. Next, we show that every non-zero element $a \in D$ is a unit. Define $\ell_a: D \rightarrow D$, $\ell_a(x) := a \cdot x$. Note that a is a unit of D if and only if 1_D is in the image of ℓ_a . We will show that ℓ_a is surjective, and in particular, its image contains 1_D . Since D is finite and ℓ_a is a function from D to D , by the pigeonhole principle, ℓ_a is surjective if and only if it is injective. So, instead of proving ℓ_a is surjective, we will argue why ℓ_a is injective. For $x_1, x_2 \in D$,

$$\ell_a(x_1) = \ell_a(x_2) \Rightarrow a \cdot x_1 = a \cdot x_2 \Rightarrow x_1 = x_2.$$

The last implication follows using the cancellation law, Lemma 19, and $a \neq 0$. This implies that ℓ_a is injective. As we explained earlier, considering ℓ_a is an injective function from a finite set to

itself, we deduce that ℓ_a is surjective. Hence, 1 is in the image of ℓ_a . This implies that a is a unit. This completes the proof. $\square$

Proposition 23. *The characteristic of an integral domain is either zero or a prime.*

Proof. Suppose to the contrary that the characteristic of an integral domain is neither zero nor prime. Recall that $\text{char}(D)$ is $\text{ord } 1_D$ if it is finite and zero otherwise. Since by the contrary assumption the characteristic $\text{char}(D) = n$ is not zero, we deduce that

$$(6) \quad \text{ord } 1_D = n.$$

The contrary assumption implies that $n > 0$ is not prime. Hence, it is either 1 or a composite number, which means $n = rs$ for some integers $r, s \geq 2$.

Case 1. $n = 1$.

In this case, $n1_D = 0_D$ implies that $1_D = 0_D$ which is a contradiction as every integral domain is non-trivial.

Case 2. $n = rs$ for some integers $r, s \geq 2$.

In this case, $n1_D = 0$ and $r1_D \neq 0$ and $s1_D \neq 0$. Note that by Proposition 10,

$$f: \mathbb{Z} \rightarrow D, \quad f(k) := k1_D$$

is a ring homomorphism. Hence,

$$f(n) = f(rs) = f(r)f(s), \quad \text{which implies that} \quad 0_D = n1_D = (r1_D)(s1_D).$$

Therefore, $r1_D$ is a zero-divisor, which contradicts the assumption that D is an integral domain. $\square$

Let's revisit $\mathbb{Z}_n$ in the light of the above results:

Corollary 24. *Suppose n is a positive integer. Then the following statements are equivalent:*

- (1) $\mathbb{Z}_n$ is an integral domain.
- (2) n is prime.
- (3) $\mathbb{Z}_n$ is a field.

Proof. (1) $\Rightarrow$ (2) The characteristic of $\mathbb{Z}_n$ is n . By Proposition 23, the characteristic of an integral domain is either 0 or prime. Since $n > 0$, we deduce that n is prime.

(2) $\Rightarrow$ (3) Since n is prime, for all $0 < a < n$, we have $\gcd(a, n) = 1$. Hence,

$$\mathbb{Z}_n^\times = \{[a]_n \mid \gcd(a, n) = 1\} = \mathbb{Z}_n \setminus \{[0]_n\}.$$

Therefore, $\mathbb{Z}_n$ is a field.

(3) $\Rightarrow$ (1) By Corollary 21, every field is an integral domain. $\square$

The first exam covers all the topics discussed up to this point.

We know that not every integral domain is a field. In order to solve linear equations, we do need to have a field. In fact, if you go over the materials that are covered in your linear algebra course, you see that everything goes through over a field: you can define the concept of dimension. You can do the reduced echelon process, etc. So, given an integral domain D , we would like to *embed* it into a field, and find *smallest* such field. Note that rational numbers are constructed out of integers through a similar desire. Having fractions in mind, we define the following relation $\sim$ on the set of pairs $D \times (D \setminus \{0\})$:

$$(a, b) \sim (a', b') \quad \text{if and only if} \quad ab' = ba'.$$

Lemma 25. *Suppose D is an integral domain. Then $\sim$ is an equivalence relation.*

Proof. (Reflexive) We must check $(a, b) \sim (a, b)$. It means $ab = ba$ which holds by commutativity of an integral domain.

(Symmetric) We must check that $(a, b) \sim (a', b')$ implies $(a', b') \sim (a, b)$. It means $ab' = ba'$ should imply $a'b = b'a$, which follows again by the commutativity of an integral domain.

(Transitive) We must show that if $(a, b) \sim (a', b')$ and $(a', b') \sim (a'', b'')$, then $(a, b) \sim (a'', b'')$. In other words, assuming $ab' = ba'$ and $a'b'' = b'a''$, we must prove that $ab'' = ba''$. Multiplying both sides of $ab' = ba'$ by b'' , we obtain

$$(7) \quad ab'b'' = ba'b''.$$

Multiplying both sides of $a'b'' = b'a''$ by b , it follows that

$$(8) \quad a'b''b = b'a''b.$$

By (7), (8), and commutativity in an integral domain, we deduce that

$$ab''b' = ba'b'' = a''bb', \quad \text{which implies} \quad (ab'')b' = (ba'')b'.$$

Hence, by the cancellation law, $ab'' = ba''$ completing the proof. $\square$

We define $+$ and $\cdot$ on the set of all the fractions as usual:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} := \frac{a_1b_2 + b_1a_2}{b_1b_2} \quad \text{and} \quad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} := \frac{a_1a_2}{b_1b_2}.$$

In the next lecture, we will discuss main properties of $(Q(D), +, \cdot)$.

5. LECTURE 5: THE UNIVERSAL PROPERTY OF FIELD OF FRACTIONS

Theorem 26 (The universal property of the field of fractions). *Suppose D is an integral domain. Let*

$$Q(D) := \left\{ \frac{a}{b} \mid a \in D, b \in D \setminus \{0\} \right\},$$

and the operations $+$ and $\cdot$ are defined as usual. Then

- (1) $+$ and $\cdot$ are well-defined.
- (2) $(Q(D), +, \cdot)$ is a field.
- (3) $i: D \rightarrow Q(D)$, $i(a) := \frac{a}{1}$ is an injective ring homomorphism.
- (4) If F is a field and $f: D \rightarrow F$ is an injective ring homomorphism such that $f(1_D) = 1_F$, then

$$\tilde{f}: Q(D) \rightarrow F, \quad \tilde{f}\left(\frac{a}{b}\right) := f(a)f(b)^{-1}$$

is a well-defined injective ring homomorphism.

- (5) $\tilde{f} \circ i = f$. We say the following diagram is commutative:

$$\begin{array}{ccc} & & Q(D) \\ & \nearrow i & \downarrow \tilde{f} \\ D & \xrightarrow{f} & F \end{array}$$

Proof. We present proofs of only parts of this theorem. Proof of the other parts follows similar ideas.

$+$ is well-defined. The issue is that a fraction is an equivalence class. Knowing a fraction does not uniquely determine its numerator and denominator. Therefore, when we define a function on fractions in terms of a chosen numerator and denominator, we must verify that the given rule

is independent of the particular representatives chosen for that fraction. Suppose $\frac{a_1}{b_1} = \frac{a'_1}{b'_1}$ and $\frac{a_2}{b_2} = \frac{a'_2}{b'_2}$. We must prove that $\frac{a_1b_2+b_1a_2}{b_1b_2} = \frac{a'_1b'_2+b'_1a'_2}{b'_1b'_2}$. Recall that

$$(9) \quad \frac{a_1}{b_1} = \frac{a'_1}{b'_1} \Leftrightarrow a_1b'_1 = b_1a'_1 \quad \text{and} \quad \frac{a_2}{b_2} = \frac{a'_2}{b'_2} \Leftrightarrow a_2b'_2 = b_2a'_2.$$

We must show $\frac{a_1b_2+b_1a_2}{b_1b_2} = \frac{a'_1b'_2+b'_1a'_2}{b'_1b'_2}$ which is equivalent to proving

$$(10) \quad (a_1b_2 + b_1a_2)(b'_1b'_2) = (b_1b_2)(a'_1b'_2 + b'_1a'_2).$$

Note that

$$\begin{aligned} (a_1b_2 + b_1a_2)(b'_1b'_2) &= a_1b_2b'_1b'_2 + b_1a_2b'_1b'_2 && \text{(by (9))} \\ &= b_1a'_1b_2b'_2 + b_2a'_2b_1b'_1 \\ &= (b_1b_2)(a'_1b'_2 + a'_2b'_1), \end{aligned}$$

which shows (10) holds.

Zero of $Q(D)$. Note that since for every $a \in D \setminus \{0\}$, $a \cdot 0 = 0 \cdot 1 = 0$, $\frac{0}{a} = \frac{0}{1}$. We also have

$$\frac{0}{1} + \frac{a}{b} = \frac{0 \cdot b + 1 \cdot a}{1 \cdot b} = \frac{a}{b}.$$

Hence, $\frac{0}{1}$ is the zero of $Q(D)$.

The identity of $Q(D)$. Note that $\frac{1}{1} \cdot \frac{a}{b} = \frac{1 \cdot a}{1 \cdot b} = \frac{a}{b}$. Hence $\frac{1}{1}$ is the identity of $Q(D)$. Moreover, for every $a \in D \setminus \{0\}$, $\frac{a}{a} = \frac{1}{1}$ as $a \cdot 1 = 1 \cdot a$.

Inverse of an element. Suppose $\frac{a}{b}$ is not zero. Then by the above argument, $a \neq 0$. Therefore, $\frac{b}{a} \in Q(D)$. Note that

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}.$$

Therefore, $(\frac{a}{b})^{-1} = \frac{b}{a}$.

Next, we prove part (3). $i(a) + i(b) = \frac{a}{1} + \frac{b}{1} = \frac{a \cdot 1 + 1 \cdot b}{1 \cdot 1} = \frac{a+b}{1} = i(a+b)$. Similarly,

$$i(a) \cdot i(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1} = i(ab).$$

Therefore, i is a ring homomorphism. Next, we show that i is injective:

$$i(a) = i(a') \Rightarrow \frac{a}{1} = \frac{a'}{1} \Rightarrow a \cdot 1 = a' \cdot 1 \Rightarrow a = a'.$$

Next, we discuss why $\tilde{f}$ is well-defined. We must prove that if $\frac{a}{b} = \frac{a'}{b'}$, then

$$f(a)f(b)^{-1} = f(a')f(b')^{-1}.$$

Note that $\frac{a}{b} = \frac{a'}{b'}$ implies $ab' = ba'$. Hence, $f(ab') = f(ba')$, which gives $f(a)f(b') = f(b)f(a')$. If $f(b)$ and $f(b')$ are non-zero, then they are units in F as F is a field. Thus

$f(a)f(b')(f(b)^{-1}f(b')^{-1}) = f(b)f(a')(f(b)^{-1}f(b')^{-1})$, which implies $f(a)f(b)^{-1} = f(a')f(b')^{-1}$, as desired. Let's point out that, since b and b' are non-zero and f is injective, $f(b)$ and $f(b')$ are non-zero. This completes the proof of well-definedness of $\tilde{f}$. It is straightforward to check that $\tilde{f}$ is a ring homomorphism.

Finally, note that for every $a \in D$,

$$\tilde{f}(i(a)) = \tilde{f}\left(\frac{a}{1_D}\right) = f(a)f(1_D)^{-1} = f(a).$$

This completes the proof of the last part. □

Exercise 2. In the above setting, use the fact that $f(1_D)^2 = f(1_D)$ and $f(1_D) \neq 0$, to show that $f(1_D) = 1_F$.

6. LECTURE 6: HOW TO USE THE UNIVERSAL PROPERTY OF FIELD OF FRACTIONS, DEFINING DEGREE, LEADING TERM AND COEFFICIENT OF POLYNOMIALS, DIVISION ALGORITHM, NILPOTENT ELEMENTS AND THEIR CONNECTION WITH UNITS.

A field isomorphic to $Q(D)$ is called a *field of fractions* of D .

Problem. Prove that $\mathbb{Q}[i] := \{a + bi \mid a, b \in \mathbb{Q}\}$ is a field of fractions of $\mathbb{Z}[i]$.

In order to show F is a field of fractions of D , we take the following steps:

- (1) Prove that F is a field.
- (2) Give an injective ring homomorphism $f: D \rightarrow F$.
- (3) Use the universal property of field of fractions and obtain the injective ring homomorphism

$$\tilde{f}: Q(D) \rightarrow F, \quad \tilde{f}\left(\frac{a}{b}\right) = f(a)f(b)^{-1}.$$

- (4) Prove that $\tilde{f}$ is surjective.

Proof. We start with showing that $\mathbb{Q}[i]$ is a subring of $\mathbb{C}$. To prove this, it is necessary and sufficient to argue why it is closed under subtraction and multiplication. For $a, b, a', b' \in \mathbb{Q}$,

$$\begin{aligned} (a + bi) - (a' + b'i) &= \underbrace{(a - a')}_{\in \mathbb{Q}} + \underbrace{(b - b')}_{\in \mathbb{Q}}i \in \mathbb{Q}[i] \\ (a + bi)(a' + b'i) &= \underbrace{(aa' - bb')}_{\in \mathbb{Q}} + \underbrace{(ab' + a'b)}_{\in \mathbb{Q}}i \in \mathbb{Q}[i]. \end{aligned}$$

Hence, $\mathbb{Q}[i]$ is a subring of $\mathbb{C}$; in particular, it is commutative. Note that $1 \in \mathbb{Q}[i]$, and so $\mathbb{Q}[i]$ is unital. To show $\mathbb{Q}[i]$ is a field, we must show that every non-zero element $a + bi$ of $\mathbb{Q}[i]$ is a unit. Note that a non-zero element of $\mathbb{C}$ is invertible and its inverse is given by

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

Note that when $a, b \in \mathbb{Q}$ and $a + bi \neq 0$, $a^2 + b^2 \neq 0$ and

$$\frac{a}{a^2 + b^2}, \frac{b}{a^2 + b^2} \in \mathbb{Q}.$$

Therefore, $(a + bi)^{-1} \in \mathbb{Q}[i]$, which implies that $a + bi \in \mathbb{Q}[i]^\times$. Altogether, we deduce that $\mathbb{Q}[i]$ is a field.

Let $f: \mathbb{Z}[i] \rightarrow \mathbb{Q}[i]$, $f(a + bi) := a + bi$. Clearly, f is an injective ring homomorphism. Therefore, by the universal property of field of fractions,

$$\tilde{f}: Q(\mathbb{Z}[i]) \rightarrow \mathbb{Q}[i], \quad \tilde{f}\left(\frac{x}{y}\right) := f(x)f(y)^{-1} = xy^{-1}$$

is a well-defined injective ring homomorphism.

It is remained to show that $\tilde{f}$ is surjective. Every element of the codomain $\mathbb{Q}[i]$ is of the form $a + bi$ where $a, b \in \mathbb{Q}$. Say

$$a = \frac{r_1}{s_1} \quad \text{and} \quad b = \frac{r_2}{s_2}.$$

Note these are fractions in $\mathbb{Q}$. Then, by a simple computation in $\mathbb{C}$,

$$a + bi = \frac{r_1 s_2 + r_2 s_1 i}{s_1 s_2} \quad (\text{note this is a fraction in complex numbers}) = (r_1 s_2 + r_2 s_1 i)(s_1 s_2)^{-1}.$$

Since $r_1, r_2 \in \mathbb{Z}$ and $s_1, s_2 \in \mathbb{Z} \setminus \{0\}$, $r_1 s_2 + r_2 s_1 i \in \mathbb{Z}[i]$ and $s_1 s_2 \in \mathbb{Z} \setminus \{0\} \subseteq \mathbb{Z}[i] \setminus \{0\}$. Therefore,

$$a + bi = \tilde{f}\left(\frac{r_1 s_2 + r_2 s_1 i}{s_1 s_2}\right).$$

This shows that $\tilde{f}$ is surjective, which completes the proof. $\square$

Let's go back to the ring of polynomials. Earlier we considered the following example:

$$([2]_6 x + [1]_6)([3]_6 x^2 + x + [1]_6) = [5]_6 x^2 + [3]_6 x + [1]_6,$$

and we remarked that, unlike the examples that you had seen in calculus for polynomials over the real numbers, the degree of the product is not the sum of the degrees. We observed that this phenomenon occurred because of the existence of zero-divisors.

Definition 9. For a polynomial $f(x) := a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in R[x]$, we say the degree of f is n if $a_n \neq 0$, and we write $\deg f = n$. The degree of the zero polynomial is defined to be $-\infty$. The leading term of f is $a_n x^n$, denoted $L(f) := a_n x^n$. The leading coefficient of f is a_n , denoted $\ell(f) := a_n$. The leading term and the leading coefficient of the zero polynomial are defined to be 0.

Lemma 27. Suppose D is an integral domain. Then for every $f, g \in D[x]$, the following statements hold:

- (1) $L(fg) = L(f)L(g)$.
- (2) $\ell(fg) = \ell(f)\ell(g)$.
- (3) $\deg fg = \deg f + \deg g$.

Proof. **Case 1.** $f = 0$.

Proof of Case 1. Note that $fg = 0$, and so $L(fg) = L(f) = \ell(fg) = \ell(f) = 0$. Then

$$L(fg) = L(f)L(g) = 0 \quad \text{and} \quad \ell(fg) = \ell(f)\ell(g) = 0.$$

We also note that $\deg(fg) = \deg(f) = -\infty$. By convention $(-\infty) + (-\infty) = (-\infty) + n = -\infty$ for all $n \in \mathbb{Z}$. Therefore,

$$\deg(fg) = \deg f + \deg g = -\infty.$$

$\square$

Case 2. $f \neq 0$ and $g \neq 0$.

Proof of Case 2. Set $f(x) = a_n x^n + \cdots + a_0$ with $a_n \neq 0$ and $g(x) = b_m x^m + \cdots + b_0$ with $b_m \neq 0$. Then

$$\begin{aligned} L(f) &= a_n x^n, & \ell(f) &= a_n, & \deg f &= n \\ L(g) &= b_m x^m, & \ell(g) &= b_m, & \deg g &= m. \end{aligned}$$

Distributing the product of $f(x)$ by $g(x)$, we obtain

$$f(x)g(x) = a_n b_m x^{n+m} + \text{terms of degree at most } n+m-1.$$

Note that, since D is an integral domain and $a_n \neq 0, b_m \neq 0$, we have $a_n b_m \neq 0$. Therefore,

$$L(fg) = a_n b_m x^{n+m}, \quad \ell(fg) = a_n b_m, \quad \text{and} \quad \deg(fg) = n+m.$$

Thus,

$$L(fg) = L(f)L(g), \quad \ell(fg) = \ell(f)\ell(g), \quad \text{and} \quad \deg fg = \deg f + \deg g.$$

$\square$

The remaining case of $f \neq 0$ and $g = 0$ follows from Case 1, by symmetry. $\square$

Corollary 28. Suppose D is an integral domain. Then the following statements hold:

- (1) $D[x]$ is an integral domain.
- (2) $D[x]^\times = D^\times$.

Proof. Since D is unital commutative, so is $D[x]$. Since D is an integral domain, $0 \neq 1$. So, it is remained to show why product of two non-zero polynomials is non-zero. Suppose $f, g \in D[x] \setminus \{0\}$. Then, $\deg f, \deg g \in \mathbb{Z}^{\geq 0}$, and so by Lemma 6,

$$\deg fg = \deg f + \deg g \neq -\infty, \quad \text{which implies that } fg \neq 0.$$

Suppose $r \in D^\times$. Then for some $s \in D$, $rs = 1$. Since $r, s \in D[x]$ and $rs = 1$, we deduce that $r \in D[x]^\times$. Therefore, $D^\times \subseteq D[x]^\times$. Next, we prove the converse inclusion.

Suppose $f \in D[x]^\times$. Then, there exists $g \in D[x]$ such that $fg = 1$. In particular, $\deg fg = 0$. By Lemma 27

$$0 = \deg f + \deg g \quad \text{since } \deg f, \deg g \in \{-\infty\} \cup \mathbb{Z}^{\geq 0}, \text{ we deduce } \deg f = \deg g = 0.$$

Hence $f, g \in D$ (are constant polynomials). Since $fg = 1$ and $f, g \in D$, it follows that $f \in D^\times$. It completes the proof. $\square$

We remark that, for some rings R , there are positive degree units in $R[x]$. For instance, $2x + 1$ is a unit in $\mathbb{Z}_8[x]$.

What do you think is special about 2 in $\mathbb{Z}_8$? That is right(!): $2^3 = 0$.

Definition 10. An element $a \in R$ is called *nilpotent* if $a^n = 0$ for some positive integer n .

For example, 2 is nilpotent in $\mathbb{Z}_8$ and $2x$ is nilpotent in $\mathbb{Z}_8[x]$ as $(2x)^3 = 0$.

How are nilpotent elements related to units? To see the connection, we must recall how we compute a geometric series:

$$\begin{aligned} S := 1 + a + a^2 + \cdots + a^{n-1} &\Rightarrow aS = a + a^2 + \cdots + a^n \\ &\Rightarrow (1 - a)S = 1 - a^n. \end{aligned}$$

This means

$$(1 - a)(1 + a + \cdots + a^{n-1}) = 1 - a^n.$$

Note that the equation holds in any unital commutative ring R . If $a^n = 0$, then

$$(1 - a)(1 + a + \cdots + a^{n-1}) = 1 \quad \text{and} \quad 1 - a, 1 + a + \cdots + a^{n-1} \in R.$$

Altogether, we deduce the following lemma:

Lemma 29. Suppose $a \in R$ is nilpotent. Then $1 - a \in R^\times$.

We also observe that if a is nilpotent, then $a^n = 0$ for some $n > 0$, which implies $(-a)^n = 0$. Therefore, $-a$ is also nilpotent. Hence, by Lemma 29,

$$a \in R \text{ nilpotent} \Rightarrow 1 + a \in R^\times.$$

The above implication together with the observation that $2x$ is nilpotent in $\mathbb{Z}_8[x]$ implies that $2x + 1 \in \mathbb{Z}_8[x]^\times$.

Another important result that you learned in your middle school about polynomials over real numbers is the long division algorithm. We recall this algorithm and try to see how much it can be extended over an arbitrary unital commutative ring.

To divide a polynomial $f(x) = a_n x^n + \cdots + a_0$ by a polynomial $g(x) = b_m x^m + \cdots + b_0$, we follow Algorithm 1. This means if $\deg f < \deg g$, we set $q = 0$ and $r = f$. Otherwise, we find a monomial cx^k such that $L(f) = L(g)(cx^k)$. Then, $f - g(cx^k)$ is of smaller degree, and we repeat this process till we end up getting a polynomial of degree smaller than g . Assuming $L(f) = a_n x^n$ and $L(g) = b_m x^m$, $L(f) = L(g)(c_k x^k)$ means

$$a_n x^n = (b_m x^m)(c_k x^k).$$

Algorithm 1 The long division algorithm

Input: $f(x), g(x) \in R[x]$
 Set $q(x) = 0$ and $r(x) = f(x)$.
while $\deg r \geq \deg g$ **do**
 Find a monomial $cx^k \in R[x]$ such that $L(r) = L(g)(cx^k)$.
 Set the new (q, r) as $(q + cx^k, r - g(cx^k))$
end while
return (q, r)

When can we do this? First, we must have $n = m + k$ for some non-negative integer k . This holds as long as $n \geq m$. Second, there should exist $c \in R$ such that $b_m c = a_n$. This equation has a solution in R if b_m is a unit in R . Note that b_m is the leading coefficient of g .

Theorem 30 (Division algorithm). *Suppose R is a unital commutative ring, $f, g \in R[x]$, and $\ell(g) \in R^\times$. Then there exists a unique pair (q, r) of polynomials such that*

$$f(x) = g(x)q(x) + r(x) \quad \text{and} \quad \deg r < \deg g.$$

Proof. (The existence part) We proceed by strong induction on $\deg f$. If $\deg f < \deg g$, then $q(x) := 0$ and $r(x) := f(x)$ satisfy the desired conditions. In particular, the base of induction follows. So, we may focus on the induction step and assume that $\deg f \geq \deg g$. Suppose $L(f) = a_n x^n$ and $L(g) = b_m x^m$. Then $n \geq m$ and $b_m \in R^\times$. Hence $(b_m^{-1} a_n) x^{n-m}$ is a monomial in $R[x]$, and

$$L(f) = L(g)((b_m^{-1} a_n) x^{n-m}) \quad \text{which implies that} \quad \deg(f(x) - g(x)((b_m^{-1} a_n) x^{n-m})) < \deg f.$$

Therefore, by the strong induction hypothesis, there exists a pair (q, r) such that

$$f(x) - g(x)((b_m^{-1} a_n) x^{n-m}) = g(x)q(x) + r(x) \quad \text{and} \quad \deg r < \deg g.$$

Thus

$$f(x) = g(x) \underbrace{((b_m^{-1} a_n) x^{n-m} + q(x))}_{q_{\text{new}}(x)} + r(x),$$

so the pair (q_{new}, r) satisfies the desired properties. This completes the proof of the existence part. (The uniqueness part) $\square$

7. LECTURE 7: DIVISION ALGORITHM, FACTOR THEOREM, GENERALIZED FACTOR THEOREM, NUMBER OF DISTINCT ZEROS OVER AN INTEGRAL DOMAIN.

Proof of the division algorithm. We went through the proof of the existence part again.

(The uniqueness part). To show the uniqueness part, we must prove if the pairs (q_1, r_1) and (q_2, r_2) satisfy the desired conditions, then $q_1 = q_2$ and $r_1 = r_2$. This means, we must prove the following implication:

$$\left. \begin{array}{l} f(x) = g(x)q_1(x) + r_1(x), \deg r_1 < \deg g \\ f(x) = g(x)q_2(x) + r_2(x), \deg r_2 < \deg g \end{array} \right\} \implies \begin{cases} g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x) \\ \deg r_1, \deg r_2 < \deg g. \end{cases}$$

Claim. $\deg(gh) = \deg g + \deg h$.

Proof of Claim. If $h = 0$, then both sides of the equation are $-\infty$. Suppose $h \neq 0$. Set $L(g) = b_m x^m$ and $L(h) = c_k x^k$. Then

$$g(x)h(x) = b_m c_k x^{m+k} + \text{terms of degree at most } m + k - 1.$$

Since $b_m \in R^\times$, it is not a zero-divisor. Knowing b_m is not a zero-divisor and $c_k \neq 0$, it follows that $b_m c_k \neq 0$. Therefore, $\deg(gh) = m + k = \deg g + \deg h$. This completes the proof of the Claim. $\square$

Hence, $\deg(g(q_1 - q_2)) = \deg g + \deg(q_1 - q_2)$, so

$$\deg g + \deg(q_1 - q_2) = \deg(r_2 - r_1).$$

Let's remark that $\deg(r_2 - r_1) \leq \max\{\deg r_2, \deg r_1\}$, and so

$$\deg(r_2 - r_1) < \deg g.$$

Altogether, we deduce that

$$\deg g + \deg(q_1 - q_2) < \deg g \quad \text{and so} \quad \deg(q_1 - q_2) < 0.$$

Thus $q_1 - q_2 = 0$, which implies that $q_1 = q_2$. Knowing that $q_1 = q_2$ and $g(q_1 - q_2) = r_2 - r_1$, we deduce that

$$r_2 - r_1 = g(q_1 - q_2) = 0, \quad \text{and so} \quad r_1 = r_2.$$

This completes the proof. $\square$

We may view a polynomial $f \in D[x]$ as a function from $R \rightarrow R$ for every ring R that contains D . Note that two different polynomials may define the same function. For example polynomials x and x^2 in $\mathbb{Z}_2[x]$ give rise to the same function from $\mathbb{Z}_2$ to $\mathbb{Z}_2$.

Warning. Two polynomials $f, g \in D[x]$ are not considered equal merely because they induce the same function $f, g: D \rightarrow D$.

Nevertheless, viewing polynomials as functions help us a lot study the ring of polynomials. Given a ring R , a subring S , and $r \in R$, *evaluation* of polynomials over S at r give us a ring homomorphism:

$$e_r: S[x] \rightarrow R, \quad e_r(f) := f(r).$$

Note that $f \in \ker e_r$ if and only if $e_r(f) = f(r) = 0$. Recall that we say r is a zero of $f(x)$ or a root of the equation $f(x) = 0$ if $f(r) = 0$. Hence

$$\ker e_r = \{f \in S[x] \mid r \text{ is a zero of } f\}.$$

Example 2. Consider $e_{\sqrt{2}}: \mathbb{Q}[x] \rightarrow \mathbb{R}$. Find $e_{\sqrt{2}}(x), e_{\sqrt{2}}(x^2 - 2), e_{\sqrt{2}}(ax + b)$. Argue why $e_{\sqrt{2}}(ax + b) \neq 0$ if $ax + b$ is not the zero polynomial.

Solution. $e_{\sqrt{2}}(x) = \sqrt{2}$. $e_{\sqrt{2}}(x^2 - 2) = \sqrt{2}^2 - 2 = 0$. $e_{\sqrt{2}}(ax + b) = a\sqrt{2} + b$. Suppose $a\sqrt{2} + b = 0$ for some $a, b \in \mathbb{Q}$. If $a \neq 0$, then $\sqrt{2} = b/a \in \mathbb{Q}$ which is a contradiction. If $a = 0$, then $a\sqrt{2} + b = 0$ implies that $b = 0$. $\square$

Problem. (1) Find the kernel of $e_{\sqrt{2}}: \mathbb{R}[x] \rightarrow \mathbb{R}$.

(2) Find the kernel of $e_{\sqrt{2}}: \mathbb{Q}[x] \rightarrow \mathbb{R}$.

Solution. (1) Over the real numbers, in your middle school you learn that c is a zero of a polynomial f if and only if f has a factor of $(x - c)$. Hence, $\sqrt{2}$ is a zero of f if and only if $f(x) = (x - \sqrt{2})q(x)$ for some $q(x) \in \mathbb{R}[x]$. So,

$$\ker e_{\sqrt{2}} = \{(x - \sqrt{2})q(x) \mid q(x) \in \mathbb{R}[x]\}.$$

(2) Note that $x - \sqrt{2} \notin \mathbb{Q}[x]$, so the answer to the second part is not the same as the first part. In fact, in the previous example, we have seen that $\ker e_{\sqrt{2}}$ has no degree 1 polynomial in $\mathbb{Q}[x]$. We have also seen that $x^2 - 2$ is in this kernel. So, maybe similar to the first part, every element of the kernel is a multiple of $x^2 - 2$.

Suppose $f \in \ker e_{\sqrt{2}}$. By the division algorithm, there exists a unique pair $(q(x), r(x)) \in \mathbb{Q}[x]$ such that

$$f(x) = q(x)(x^2 - 2) + r(x) \quad \text{and} \quad \deg r < \deg(x^2 - 2).$$

Note that the leading coefficient of $x^2 - 2$ is 1, and so it is a unit. (a polynomial is called *monic* if its leading coefficient is 1) Therefore, we may apply the division algorithm theorem. Since $\deg r < 2$,

$r(x) = ax + b$ for some $a, b \in \mathbb{Q}$. Evaluating both sides of $f(x) = q(x)(x^2 - 2) + ax + b$ at $\sqrt{2}$, we deduce that

$$0 = f(\sqrt{2}) = q(\sqrt{2})(\sqrt{2}^2 - 2) + a\sqrt{2} + b \quad \text{which implies that} \quad a\sqrt{2} + b = 0.$$

Using the previous example, it follows that $a = b = 0$, and so $r(x) = 0$. Thus $f(x) = (x^2 - 2)q(x)$ for some $q(x) \in \mathbb{Q}[x]$. This shows that

$$\ker e_{\sqrt{2}} = \{(x^2 - 2)q(x) \mid q(x) \in \mathbb{Q}[x]\}.$$

□

A major part of this course is extending this result. We will be using the same idea: taking a polynomial m_α of smallest degree that has α as a zero. Dividing a polynomial f that has α as a zero by m_α : $f(x) = m_\alpha(x)q(x) + r(x)$ and $\deg r < \deg m_\alpha$. Evaluating both sides at α and deducing that $r(\alpha) = 0$. Using the assumption that $\deg m_\alpha$ is smallest among non-zero polynomials that have α as a zero, and deducing that $r(x) = 0$, and so f is a multiple of m_α .

Theorem 31 (Factor theorem). *Suppose R is a unital commutative ring and $c \in R$. Then for every $f \in R[x]$, there exists $q \in R[x]$ such that*

$$f(x) = (x - c)q(x) + f(c).$$

In particular, c is a zero of f if and only if there exists $q(x) \in R[x]$ such that $f(x) = (x - c)q(x)$.

Proof. Since $x - c$ is a monic polynomial (that means the leading coefficient is 1), we may apply the division algorithm. Hence, there exists a pair $(q, r) \in R[x]$ such that

$$f(x) = (x - c)q(x) + r(x) \quad \text{and} \quad \deg r < \deg(x - c).$$

The inequality implies that r is a constant polynomial. Evaluating both sides of $f(x) = (x - c)q(x) + r$ at c , we deduce that $r = f(c)$. Therefore, $f(x) = (x - c)q(x) + f(c)$.

If c is a zero of f , then $f(x) = (x - c)q(x) + f(c)$ implies that $f(x) = (x - c)q(x)$.

If $f(x) = (x - c)q(x)$, then $f(c) = 0$. This completes the proof. □

Note that the factor theorem implies for every $c \in R$,

$$\ker e_c = \{(x - c)q(x) \mid q(x) \in R[x]\}.$$

Over the real numbers, having other zeros of a polynomial f , you could find a factorization of f . **Can we do the same over an arbitrary ring? Under what condition can we do it?**

Suppose $c_1, \dots, c_n \in R$ are distinct zeros of a polynomial $f \in R[x]$. By the factor theorem, $f(x) = (x - c_1)q(x)$. Now, we wish to factor $f(x)$ further, and for that we must factor q . Do we know a zero of q ? Is c_2 a zero of q ? Let's evaluate both sides of $f(x) = (x - c_1)q(x)$ at c_2 . We deduce that

$$0 = f(c_2) = (c_2 - c_1)q(c_2).$$

Note that $c_2 - c_1 \neq 0$ as c_i 's are distinct zeros of f . Can we deduce that $q(c_2) = 0$. That is right(!), we can do so only when R has no zero-divisors. This takes us to the next theorem:

Theorem 32 (Generalized factor theorem). *Suppose D is an integral domain, $f \in D[x]$, and $c_1, \dots, c_n \in D$ are distinct zeros of f . Then there exists $q \in R[x]$ such that*

$$f(x) = (x - c_1) \cdots (x - c_n)q(x).$$

Proof. We proceed by induction on n . The base case follows from the Factor theorem.

The induction step. Since c_1 is a zero of f , by the Factor theorem, there exists $g(x) \in D[x]$ such that

$$(11) \quad f(x) = (x - c_1)g(x).$$

For every $2 \leq i \leq n$, $0 = f(c_i) = (c_i - c_1)g(c_i)$. Since $c_i - c_1 \neq 0$ and D has no zero-divisors, $(c_i - c_1)g(c_i) = 0$ implies that $g(c_i) = 0$ for $2 \leq i \leq n$. By the induction hypothesis, there exists $q(x) \in D[x]$,

$$(12) \quad g(x) = (x - c_2) \cdots (x - c_n)q(x).$$

Therefore, by (11) and (12),

$$f(x) = (x - c_1)(x - c_2) \cdots (x - c_n)q(x).$$

This completes the proof. $\square$

For a polynomial $f \in D[x]$, let $V_f(D)$ be the set of zeros of f in D ; that means

$$V_f(D) := \{a \in D \mid f(a) = 0\}$$

Corollary 33. *Suppose D is an integral domain. Then for every $f \in D[x] \setminus \{0\}$,*

$$|V_f(D)| \leq \deg f.$$

This means the number of distinct zeros of f in D is at most equal to the degree of f .

Proof. Suppose $V_f(D) = \{c_1, \dots, c_n\}$ and c_i 's are distinct. Then by the generalized factor theorem, there exists $q(x) \in D[x]$ such that

$$f(x) = (x - c_1) \cdots (x - c_n)q(x).$$

Since $f \neq 0$, $q \neq 0$. Hence, $\deg q \geq 0$. As D is an integral domain,

$$\deg f = \deg(x - c_1) + \cdots + \deg(x - c_n) + \deg q = n + \deg q \geq n.$$

This completes the proof. $\square$

8. LECTURE 8: ZEROS OF POLYNOMIALS IN DIRECT PRODUCTS, FERMAT'S LITTLE THEOREM, FROBENIUS HOMOMORPHISM, FACTORIZATION OF $x^p - x$ OVER $\mathbb{Z}_p$, WILSON'S THEOREM, IRREDUCIBLE ELEMENTS, IRREDUCIBLE POLYNOMIALS OVER A FIELD, HAVING ZERO AND FACTORIZATION, DEGREE 2 OR 3 IRREDUCIBILITY CRITERION.

In the previous lecture, we proved that a polynomial of degree n over an integral domain does not have more than n distinct zeros. The following are immediate consequences of this result:

Corollary 34. *Suppose D is an integral domain and $a_1, \dots, a_{n+1} \in D$ are distinct. Suppose $f, g \in D[x]$ and $\deg f, \deg g \leq n$. Then $f = g$ if and only if $f(a_i) = g(a_i)$ for all $i = 1, \dots, n+1$.*

Proof. Let $h(x) := f(x) - g(x)$. Then $\deg h \leq n$ and it has at least $n+1$ distinct zeros. By Corollary 33, we deduce that $h = 0$, and so $f(x) = g(x)$. This completes the proof. $\square$

We remarked that it is not enough to know two polynomials of degree n are equal only at n points in order to deduce they are equal. For instance, every polynomial of the form $c(x-1)$ is 0 at 1, but they are not equal to each other. In terms of graph of functions, graph of a polynomial of degree 1 is a line, and knowing that $f(1) = 0$ only implies that the graph of f is a line which passes through the point $(1, 0)$. This information does not specify a unique line. On the other hand, if we know two points, then we obtain a unique line passing through them. The above corollary shows that if graph of two polynomials of degree at most n pass through the same $n+1$ points, then they are identical polynomials.

Example 3. Find $V_{2x^2-x}(R)$ where $R = \mathbb{Q}$, $\mathbb{Z}$, and $R = \mathbb{Z}_{15}$.

Solution. Let's start with $R = \mathbb{Q}$. We must solve the equation

$$2x^2 - x = 0$$

Note that $2x^2 - x = x(2x - 1)$. Since $\mathbb{Q}$ is an integral domain, $x(2x - 1) = 0$ implies that either $x = 0$ or $2x - 1 = 0$. Hence $V_{2x^2-x}(\mathbb{Q}) = \{0, 1/2\}$.

Since $\mathbb{Z}$ is a subring of $\mathbb{Q}$, we may use our previous result and see which ones are integer. We see that $V_{2x^2-x} = \{0\}$ **Not all rational roots are integer!**

Why can we not use the same argument for the ring $\mathbb{Z}_{15}$? That is right! Since $\mathbb{Z}_{15}$ has zero divisors, $x(2x - 1) = 0$ does not imply that one of the factors must be zero. By the Chinese Remainder Theorem, $\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$. Hence, we must find $V_{2x^2-x}(\mathbb{Z}_3 \times \mathbb{Z}_5)$. Set $f(x) := 2x^2 - x$, and observe that

$$f(a, b) = (f(a), f(b)).$$

Therefore, (a, b) is a zero of f if and only if a and b are zeros of f . Thus

$$V_{2x^2-x}(\mathbb{Z}_3 \times \mathbb{Z}_5) = V_{2x^2-x}(\mathbb{Z}_3) \times V_{2x^2-x}(\mathbb{Z}_5).$$

Since $\mathbb{Z}_3$ and $\mathbb{Z}_5$ are integral domains, we may apply the same logic as in the case of rational numbers and deduce that for every odd prime p

$$V_{2x^2-x}(\mathbb{Z}_p) = \{0, [2]_p^{-1}\}.$$

Note that $[2]_3^{-1} = [2]_3$ and $[2]_5^{-1} = [3]_5$. Therefore,

$$V_{2x^2-x}(\mathbb{Z}_{15}) = \{([0]_3, [0]_5), ([0]_3, [3]_5), ([2]_3, [0]_5), ([2]_3, [3]_5)\}.$$

In order to go back to $\mathbb{Z}_{15}$, we must find all $[x]_{15}$ such that $([x]_3, [x]_5)$ is one of the above pairs.

For small numbers $p < q$ in order to find $[x]_{pq}$ such that $[x]_p = [a]_p$ and $[y]_q = [b]_q$, we may go over the arithmetic progression $b, b + q, \dots, b + (p - 1)q$ and find out which one satisfies the condition $[b + kq]_p = [a]_p$. For large p and q , it is more efficient to use the Euclidean algorithm.

Using the above strategy, we can find:

$$([0]_3, [0]_5) \mapsto [0]_{15}, \quad ([0]_3, [3]_5) \mapsto [3]_{15}, \quad ([2]_3, [0]_5) \mapsto [5]_{15}, \quad ([2]_3, [3]_5) \mapsto [8]_{15}.$$

Therefore,

$$V_{2x^2-x}(\mathbb{Z}_{15}) = \{0, 3, 5, 8\}.$$

Note that a degree 2 polynomial might have more than two distinct zeros over a ring which is not an integral domain. $\square$

Example 4. Find $V_{x^p-x}(\mathbb{Z}_p)$.

Solution. To answer this question, we must recall Fermat's little theorem.

Theorem 35 (Fermat's little theorem). *for every $a \in \mathbb{Z}$, $a^p \equiv a$.*

We will present two proofs for Fermat's little theorem. Before doing so, we show how to answer the above question using this theorem.

By Fermat's little theorem, every element of $\mathbb{Z}_p$ is a zero of $x^p - x$. Hence

$$V_{x^p-x}(\mathbb{Z}_p) = \{[0]_p, \dots, [p-1]_p\}.$$

$\square$

An important consequence of the above examples is the following theorem.

Theorem 36. $x^p - x = x(x - 1) \cdots (x - p + 1)$ in $\mathbb{Z}_p[x]$.

Proof. By the previous example, $0, \dots, p-1$ are zeros of $x^p - x$. Since $\mathbb{Z}_p$ is an integral domain, we may apply the Generalized Factor Theorem, and deduce

$$x^p - x = x(x-1) \cdots (x-(p-1))q(x)$$

for some $q(x) \in \mathbb{Z}_p[x]$. Comparing the degrees of both sides, we obtain

$$p = p + \deg q \quad \text{which implies} \quad \deg q = 0.$$

Hence $q(x) = c \in \mathbb{Z}_p \setminus \{0\}$, which means

$$x^p - x = cx(x-1) \cdots (x-(p-1)).$$

Comparing the leading coefficients of both sides, it follows that $1 = c$. Thus

$$x^p - x = x(x-1) \cdots (x-(p-1)) \quad \text{in } \mathbb{Z}_p[x].$$

This completes the proof. $\square$

Corollary 37 (Wilson's theorem). *For every prime p , $(p-1)! \equiv -1$.*

Proof. Comparing the coefficient of x on both sides of

$$x^p - x = x(x-1) \cdots (x-(p-1))$$

we deduce that

$$-1 = (-1)(-2) \cdots (-(p-1)) \quad \text{in } \mathbb{Z}_p.$$

The right hand side equals $(-1)^{p-1}(p-1)!$. If p is odd, $(-1)^{p-1} = 1$. If $p = 2$, then $-1 \equiv 1$. So, in either case, we obtain

$$-1 \equiv (p-1)!.$$

$\square$

Let's go back to the proof of Fermat's little theorem. We present two proofs. The first one is based on group theory and the second one is based on ring theory.

Proof of Fermat's little theorem using group theory. By Lagrange's theorem, order of every element of a finite group divides the order of the group. So, for every $a \in \mathbb{Z}_n^\times$, $a^{|\mathbb{Z}_n^\times|} = 1$. Recall that $|\mathbb{Z}_n^\times| = \phi(n)$. Hence

$$a^{\phi(n)} \equiv 1 \quad \text{if } \gcd(a, n) = 1.$$

This is known as Euler's theorem. For $n = p$, we have $\phi(p) = |\mathbb{Z}_p^\times| = |\mathbb{Z}_p \setminus \{0\}| = p-1$. Hence, if $[a]_p \neq 0$, then

$$[a]_p^{p-1} = [1]_p, \quad \text{which implies that} \quad [a]_p^p = [a]_p.$$

The last equation clearly holds for $[a]_p = 0$. This completes the proof of Fermat's little theorem. $\square$

Proof of Fermat's little theorem using ring theory. The main tool is the *Frobenius homomorphism*.

Proposition 38. *Suppose R is a unital commutative ring of characteristic p where p is prime. Let $F: R \rightarrow R$, $F(r) := r^p$. Then F is a ring homomorphism.*

Proof. We must show that, for every $r_1, r_2 \in R$,

$$F(r_1 r_2) = F(r_1)F(r_2) \quad \text{and} \quad F(r_1 + r_2) = F(r_1) + F(r_2).$$

Note that $F(r_1 r_2) = (r_1 r_2)^p$ which is equal to $r_1^p r_2^p$ as R is commutative. To show the second equation, we use the binomial expansion.

Let's recall that

$$(x+y)^n = \underbrace{(x+y) \cdots (x+y)}_{n \text{ times}}.$$

We distribute. From each factor, we may choose either x or y . Suppose we choose x from i of the parentheses and y from the remaining ones. In this way we obtain the monomial $x^i y^{n-i}$. The number of times this monomial is achieved equals the number of ways to choose i factors out of the n factors. The number of choosing i out of n candidates is denoted by $\binom{n}{i}$, read as n choose i . Therefore,

$$(x + y)^n = \sum_{i=0}^n \binom{n}{i} x^i y^{n-i}.$$

To choose i , first we take a permutation and take the first i . Permuting the first i and the last $n - i$ results to the same choice of i . Hence,

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}.$$

We have

$$F(r_1 + r_2) = (r_1 + r_2)^p = \sum_{i=0}^p \binom{p}{i} r_1^i r_2^{p-i}.$$

Note that for every $1 \leq i \leq p-1$, $\gcd(p, i!(p-i)!) = 1$. Therefore, $p \mid \binom{p}{i}$ if $1 \leq i \leq p-1$. Since the characteristic of R is p , for every $r \in R$, $pr = 0$. Hence, for every $r \in R$ and $1 \leq i \leq p-1$, $\binom{p}{i}r = 0$. This implies that for all $r_1, r_2 \in R$ and $1 \leq i \leq p-1$,

$$\binom{p}{i} r_1^i r_2^{p-i} = 0.$$

Hence,

$$F(r_1 + r_2) = (r_1 + r_2)^p = \sum_{i=0}^p \binom{p}{i} r_1^i r_2^{p-i} = \underbrace{r_2^p}_{i=0} + \underbrace{r_1^p}_{i=p} = F(r_1) + F(r_2).$$

This completes the proof. $\square$

Note that $\mathbb{Z}_p$ is of characteristic p . Hence, $F: \mathbb{Z}_p \rightarrow \mathbb{Z}_p, F(a) := a^p$ is a ring homomorphism. For every $a \in \mathbb{Z}_p$,

$$a^p = F(a) = F(\underbrace{1 + \cdots + 1}_{a \text{ times}}) = \underbrace{F(1) + \cdots + F(1)}_{a \text{ times}} = \underbrace{1 + \cdots + 1}_{a \text{ times}} = a.$$

This completes the proof of Fermat's little theorem. $\square$

Definition 11. Suppose D is an integral domain. We say $a \in D$ is *irreducible* if

- (1) $a \notin \{0\} \cup D^\times$.
- (2) $a = bc$ implies either $b \in D^\times$ or $c \in D^\times$.

An irreducible element is *unbreakable* from multiplicative point of view. Note that if $b \in D^\times$, then for every $a \in D$, $a = b(b^{-1}a)$. So, these type of factorizations cannot be avoided. An irreducible has no non-trivial factorization.

Example 5. An element of $\mathbb{Z}$ is irreducible if and only if it is of the form $\pm p$ where p is a prime (in classical sense).

Question. Suppose F is a field. What can we say about irreducible elements of $F[x]$?

Solution. Note that $F[x]^\times = F^\times = F \setminus \{0\}$. So $f \notin \{0\} \cup F[x]^\times$ is equivalent to saying that $f \notin F$, and this is the same as having $\deg f \geq 1$.

If $\deg f \geq 1$ and f is not irreducible, then there exist $g, h \in F[x]$ that are not unit and $f = gh$. Since $F[x]^\times = F \setminus \{0\}$, $g, h \notin F[x]^\times$, and they are non-zero, $\deg g, \deg h \geq 1$. Which means f can be written as a product of two polynomials of positive degree.

Conversely, if a polynomial f can be written as product of polynomials of positive degree, then f cannot be irreducible as positive degree polynomials in $F[x]$ are not units. Altogether, we have proved:

Proposition 39. *Suppose F is a field. Then $f \in F[x]$ is irreducible if and only if $\deg f \geq 1$ and f cannot be written as a product of positive degree polynomials.*

□

Corollary 40. *Suppose F is a field. Then every polynomial of degree 1 in $F[x]$ is irreducible.*

Proof. Product of two polynomials of positive degree is of degree at least $1 + 1 = 2$. Hence, a degree 1 polynomial over a field is irreducible. □

Example 6. Is $2x$ irreducible in $\mathbb{Z}[x]$?

Solution. Note that $\mathbb{Z}[x]^\times = \mathbb{Z}^\times = \{1, -1\}$. Hence, $2, x \notin (\mathbb{Z}[x])^\times$. Therefore, $2x = (2)(x)$ is a non-trivial factorization, which implies that $2x$ is not irreducible in $\mathbb{Z}[x]$. □

Note that $2x$ is irreducible in $\mathbb{Q}[x]$, but it is not irreducible in $\mathbb{Z}[x]$.

Suppose $c \in F$ is a zero of a polynomial $f \in F[x]$. Then by the Factor Theorem, there exists $q \in F[x]$ such that

$$f(x) = (x - c)q(x).$$

In particular, $\deg q = \deg f - 1$. So, if $\deg f \geq 2$ and it has a zero in F , then it can be written as a product of two positive degree polynomials in $F[x]$. Therefore, it is not irreducible. Let's summarize this result.

Proposition 41. *Suppose F is a field and $f \in F[x]$. If $\deg f \geq 2$ and f has a zero in F , then f is not irreducible in $F[x]$.*

In this course, we will prove certain irreducibility criteria. The first one is a converse of Proposition 41 for polynomials of degree 2 or 3.

Theorem 42 (Degree 2 or 3 irreducibility criterion). *Suppose F is a field and $f \in F[x]$. Suppose $\deg f = 2$ or 3 . Then f is irreducible if and only if f has no zero.*

Proof. We prove the contrapositive of both directions.

Proposition 41 proves that having zero for $\deg f = 2$ or 3 implies reducibility.

Suppose f is not irreducible. Then f can be written as a product gh of polynomials of positive degree. Since $\deg f = \deg g + \deg h$, we deduce that

$$2 \leq \deg g + \deg h \leq 3.$$

Hence, the smaller one is 1. Suppose $g(x) = ax + b$ and $a \in F \setminus \{0\}$. Then $-ba^{-1} \in F$ is a zero of f . □

9. LECTURE 9: RATIONAL ROOT CRITERION AND ITS APPLICATIONS. NO ZERO MOD p IMPLIES NO RATIONAL ZERO. CONTENT OF A POLYNOMIAL AND ITS BASIC PROPERTIES.

Is it easy to find out if a polynomial has a zero in F ? Let's start with $F = \mathbb{Q}$.

Theorem 43 (Rational root criterion). *Suppose $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$, $a_n \neq 0$. Suppose $\frac{r}{s}$ is a simplified rational number; that is $\gcd(r, s) = 1$. If $\frac{r}{s}$ is a zero of f , then*

$$r | a_0 \quad \text{and} \quad s | a_n.$$

Proof. Since $\frac{r}{s}$ is a zero of f ,

$$a_n\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0 = 0.$$

Multiplying both sides by s^n , it follows that

$$a_nr^n + a_{n-1}r^{n-1}s + \cdots + a_{n-i}r^{n-i}s^i + \cdots + a_0s^n = 0.$$

Therefore,

$$\begin{aligned} -a_nr^n &= s(a_{n-1}r^{n-1} + \cdots + a_{n-i}r^{n-i}s^{i-1} + \cdots + a_0s^{n-1}) \\ -a_0s^n &= r(a_nr^{n-1} + a_{n-1}r^{n-2}s + \cdots + a_{n-i}r^{n-i-1}s^i + \cdots + a_1s^{n-1}). \end{aligned}$$

Hence, $s|a_0r^n$ and $r|a_ns^n$. Since $\gcd(r, s) = 1$, by Euclid's lemma, we deduce

$$s|a_0 \quad \text{and} \quad r|a_n.$$

This completes the proof. $\square$

Recall that a polynomial is called *monic* if its leading coefficient is 1.

Corollary 44. *Suppose $f \in \mathbb{Z}[x]$ is a monic polynomial. Then $V_f(\mathbb{Q}) = V_f(\mathbb{Z})$; that means every rational zero of f is an integer.*

Proof. Suppose $\frac{r}{s}$ is a zero of f and $\gcd(r, s) = 1$. Then by the rational root criterion, $s|1$. Hence, $s = \pm 1$. Therefore, $\frac{r}{s}$ is an integer. $\square$

Example 7. Does $f(x) := x^{50} - x^{20} + 103x + 1$ has a zero in rational numbers?

Answer. Suppose $\frac{r}{s}$ is a zero of f and $\gcd(r, s) = 1$. Then by the rational root criterion, $r, s|1$. Hence, $\frac{r}{s}$ is either 1 or -1 . Note that $f(1) = 104$ and $f(-1) = 104$. Therefore, f has no zero in rational numbers. $\square$

Example 8. Suppose $f(x) \in \mathbb{Z}[x]$ is monic and its constant term is 1; that is equivalent to say $f(0) = 1$. Then $V_f(\mathbb{Q}) \subseteq \{1, -1\}$; that is to say a zero of f in $\mathbb{Q}$ is either 1 or -1 .

Proof. Suppose $\frac{r}{s}$ is a zero of f and $\gcd(r, s) = 1$. Then by the rational root criterion, $r|f(0)$ and $s|\ell(f)$. By our assumptions, both r and s divide 1. Thus $r = \pm 1$ and $s = \pm 1$, so $\frac{r}{s} = \pm 1$. $\square$

When the leading coefficient and the constant term have many divisors, computing the polynomial is not straightforward, and other techniques are needed. Note that computations in $\mathbb{Z}_p$ are much easier to carry out than those in $\mathbb{Q}$. So, it might be easier to show $V_f(\mathbb{Z}_p) = \emptyset$. Does this help us with $V_f(\mathbb{Q})$?

Theorem 45. *Suppose $f \in \mathbb{Z}[x]$ is a monic polynomial. If $V_f(\mathbb{Z}_p) = \emptyset$ for some prime p , then $V_f(\mathbb{Q}) = \emptyset$. This means having no zero in $\mathbb{Z}_p$ implies having no zero in $\mathbb{Q}$.*

Strategy of proof: We prove the contrapositive.

- (1) (Passing from $\mathbb{Q}$ to $\mathbb{Z}$) $V_f(\mathbb{Q}) \neq \emptyset$ implies that $V_f(\mathbb{Z}) \neq \emptyset$.
- (2) (Passing from $\mathbb{Z}$ to $\mathbb{Z}_p$) Using the residue map modulo p to show $V_f(\mathbb{Z}) \neq \emptyset$ implies $V_f(\mathbb{Z}_p) \neq \emptyset$.

To be more precise, we must say $V_{c_p(f)}(\mathbb{Z}_p)$ where

$$c_p: \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x], \quad c_p(a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0) := c_p(a_n)x^n + c_p(a_{n-1})x^{n-1} + \cdots + c_p(a_0)$$

is the ring homomorphism given by the residue map modulo p .

Proof. We prove the contrapositive of the statement. Suppose f has a zero in $\mathbb{Q}$. Then by Corollary 44, f has a zero in $\mathbb{Z}$ as f is monic. Suppose $a \in \mathbb{Z}$ is a zero of f . Then, if

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

then

$$\begin{aligned} a^n + a_{n-1}a^{n-1} + \cdots + a_0 &= 0 && \text{which implies} \\ c_p(a^n + a_{n-1}a^{n-1} + \cdots + a_0) &= 0 && \text{and so} \\ c_p(a)^n + c_p(a_{n-1})c_p(a)^{n-1} + \cdots + c_p(a_0) &= 0. && \text{Hence} \\ c_p(f)([a]_p) &= 0. \end{aligned}$$

Therefore, $[a]_p \in V_f(\mathbb{Z}_p)$ (it is more precise to say $[a]_p \in V_{c_p(f)}(\mathbb{Z}_p)$). This completes the proof. $\square$

We mentioned that it is easier to do computations in $\mathbb{Z}_p$ compared to $\mathbb{Z}$. Here is one example: over $\mathbb{Z}$ it is not that easy to find powers of numbers, but modulo a prime p it is much easier thanks to Fermat's little theorem.

By Fermat's little theorem, for every prime p and every positive integer n , we have

$$a^{p^n} = a$$

for all $a \in \mathbb{Z}_p$. Therefore,

$$a^{c_n p^n + c_{n-1} p^{n-1} + \cdots + c_0} = a^{c_n + \cdots + c_0}$$

for all $a \in \mathbb{Z}_p$.

Problem. Compute $2^{51} \pmod{5}$.

Solution. We write 51 in base 5: $51 = 2 \cdot 5^2 + 1$. Hence for all $a \in \mathbb{Z}_5$,

$$a^{51} = a^{2 \cdot 5^2 + 1} = a^{2+1} = a^3.$$

Hence

$$2^{51} \stackrel{5}{\equiv} 2^3 \stackrel{5}{\equiv} 3.$$

$\square$

Problem. Show that $f(x) := x^{51} - x^3 + 103$ has no zero in $\mathbb{Z}_5$. Prove that f has no zero in $\mathbb{Q}$.

Solution. Note that for all $a \in \mathbb{Z}_5$,

$$a^{51} - a^3 + 103 = a^{2 \cdot 5^2 + 1} - a^3 + 3 = a^3 - a^3 + 3 = 3 \neq 0.$$

Hence, there is no $a \in \mathbb{Z}_p$ for which $f(a) = 0$; this means $V_f(\mathbb{Z}_5) = \emptyset$. By Theorem 45, we deduce that f has no zero in $\mathbb{Q}$. $\square$

Problem. Prove that $f(x) := x^{49} - 7x^{10} - 8x + 15$ has no zero in $\mathbb{Q}$.

Solution. As the powers suggest, it might be a good idea to first test if f has a zero in $\mathbb{Z}_7$. For every $a \in \mathbb{Z}_7$, using Fermat's little theorem, we have

$$a^{49} - 7a^{10} - 8a + 15 = a - a + 1 = 1 \neq 0.$$

Hence, $V_f(\mathbb{Z}_7) = \emptyset$. Therefore, by Theorem 45, $V_f(\mathbb{Q}) = \emptyset$, which means f has no zero in $\mathbb{Q}$. $\square$

Problem. Suppose $f \in \mathbb{R}[x]$, $\deg f \geq 3$ and it is odd. Prove that f is not irreducible in $\mathbb{R}[x]$.

Solution. Note if the leading coefficient of f is positive, $\lim_{x \rightarrow \infty} f(x) = \infty$ and $\lim_{x \rightarrow -\infty} f(x) = -\infty$. Hence, by the intermediate value theorem, $f(c) = 0$ for some real value c . This means f has a zero in real numbers. By Proposition 41, we deduce that f is not irreducible in $\mathbb{R}[x]$. $\square$

Theorem 46 (Mod- p irreducibility criterion). *Suppose $f \in \mathbb{Z}[x]$ is a monic polynomial. If f is irreducible in $\mathbb{Z}_p[x]$ for some prime p , then f is irreducible in $\mathbb{Q}[x]$.*

Strategy of the proof. It is similar to Theorem 45. We prove the contrapositive.

- (1) (Passing from $\mathbb{Q}$ to $\mathbb{Z}$) Having a factorization over $\mathbb{Q}$, we will find a factorization over $\mathbb{Z}$.
- (2) (Going from $\mathbb{Z}$ to $\mathbb{Z}_p$) Using the residue map modulo p to obtain a factorization over $\mathbb{Z}_p$.

To carry out the first step, we prove Gauss's lemma, which is based on the *content of a polynomial*.

Definition 12. Suppose $f := a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \setminus \{0\}$. Let

$$\alpha(f) := \gcd(a_n, a_{n-1}, \dots, a_0).$$

The quantity $\alpha(f)$ is called the *content* of f . A polynomial is called *primitive* if its content is 1.

Example 9. (1) $\alpha(2x^2 + 4) = 2$.

(2) $\alpha(6x^2 - 9x - 15) = 3$.

(3) Suppose $f \in \mathbb{Z}[x]$ is a monic polynomial. Then $\alpha(f) = 1$, and so it is a primitive polynomial.

To capture basic properties of content of a polynomial, we recall basic properties of gcd of numbers.

Proposition 47. *Suppose $a_0, \dots, a_n \in \mathbb{Z}$ and not all of them are zero. The greatest common divisor of a_i 's is denoted by*

$$\gcd(a_0, \dots, a_n).$$

(1) Suppose $d := \gcd(a_0, \dots, a_n)$. Then

$$\gcd\left(\frac{a_0}{d}, \dots, \frac{a_n}{d}\right) = 1.$$

(2) Suppose $c \in \mathbb{Z} \setminus \{0\}$. Then

$$\gcd(ca_0, \dots, ca_n) = |c| \gcd(a_0, \dots, a_n).$$

(3) Suppose p is a prime number. Then $c \mid \gcd(a_0, \dots, a_n)$ if and only if for all i , $c_p(a_i) = 0$.

Next, we examine the consequences of the properties of gcd listed in Proposition 47 for the content of polynomials.

Proposition 48 (Basic properties of content). (1) *For every $f \in \mathbb{Z}[x] \setminus \{0\}$, $\alpha(f)^{-1}f(x)$ is a primitive polynomial. It is denoted by f_{prim} , and we call it the primitive factor of f . So, $f(x) = \alpha(f)f_{\text{prim}}(x)$ and f_{prim} is primitive.*

(2) *For every $c \in \mathbb{Z} \setminus \{0\}$ and non-zero polynomial $f \in \mathbb{Z}[x]$, $\alpha(cf) = |c|\alpha(f)$.*

(3) *For every prime p and non-zero polynomial $f \in \mathbb{Z}[x]$, we have*

$$p \mid \alpha(f) \iff c_p(f) = 0,$$

where $c_p: \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ is the residue map modulo p .

Proof. (1) Suppose $f(x) = a_n x^n + \cdots + a_0$ and $\alpha(f) = d$. Then by the first part of Proposition 47, $a_i = da'_i$ for all i and

$$\gcd(a'_n, \dots, a'_0) = 1.$$

Hence, the polynomial $f_{\text{prim}}(x) := a'_n x^n + \cdots + a'_0$ is a primitive polynomial and

$$f(x) = a_n x^n + \cdots + a_0 = da'_n x^n + \cdots + da'_0 = d(a'_n x^n + \cdots + a'_0) = df_{\text{prim}}(x) = \alpha(f)f_{\text{prim}}(x).$$

(2) Suppose $f(x) = a_n x^n + \cdots + a_0$. Then by the second part of Proposition 47,

$$\gcd(ca_n, \dots, ca_0) = |c| \gcd(a_n, \dots, a_0) = |c|\alpha(f).$$

Hence, $\alpha(cf) = |c|\alpha(f)$.

- (3) Suppose $f(x) = a_n x^n + \cdots + a_0$. Note that by part (3) of Proposition 47,

$$p|\alpha(f) \iff p|\gcd(a_n, \dots, a_0) \iff \forall i, c_p(a_i) = 0 \iff c_p(f) = 0.$$

This completes the proof. $\square$

10. LECTURE 10: GAUSS'S LEMMA, VERSIONS 1,2, AND 3. MOD- p IRREDUCIBILITY CRITERION. EISENSTEIN'S IRREDUCIBILITY CRITERION.

Lemma 49 (Gauss's lemma, version 1). *Product of two primitive polynomials is primitive.*

Proof. Suppose to the contrary that there exist $f, g \in \mathbb{Z}[x]$ such that f and g are primitive, but fg is not primitive. Hence, $\alpha(fg) \neq 1$. Therefore, there exists a prime p such that $p|\alpha(fg)$. By Part (3) of Proposition 48, $c_p(fg) = 0$, where

$$c_p: \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x], \quad c_p\left(\sum_{i=0}^n a_i x^i\right) := \sum_{i=0}^n [a_i]_p x^i.$$

Since c_p is a ring homomorphism,

$$(13) \quad c_p(f)c_p(g) = 0.$$

Since p is prime, $\mathbb{Z}_p$ is an integral domain. Thus, by Corollary 28, $\mathbb{Z}_p[x]$ is an integral domain. Therefore, by (13), it follows that

$$c_p(f) = 0 \quad \text{or} \quad c_p(g) = 0.$$

By Part(3) of Proposition 48, we deduce that

$$(14) \quad p|\alpha(f) \quad \text{or} \quad p|\alpha(g).$$

Since f and g are primitive, $\alpha(f) = \alpha(g) = 1$. Thus, by (14), p has to divide 1, which is a contradiction. This completes the proof. $\square$

Lemma 50 (Gauss's lemma, version 2). *For every $f, g \in \mathbb{Z}[x] \setminus \{0\}$, $\alpha(fg) = \alpha(f)\alpha(g)$.*

Proof. By Part(1) of Proposition 48,

$$(15) \quad f(x) = \alpha(f)f_{\text{prim}}(x) \quad \text{and} \quad g(x) = \alpha(g)g_{\text{prim}}(x),$$

and f_{prim} and g_{prim} are primitive. By (15), we deduce that

$$(16) \quad f(x)g(x) = \alpha(f)\alpha(g)f_{\text{prim}}(x)g_{\text{prim}}(x).$$

Comparing the contents of both sides of the equation given in (16), we obtain

$$(17) \quad \alpha(fg) = \underbrace{\alpha(f)\alpha(g)}_{\in \mathbb{Z}^+} f_{\text{prim}}g_{\text{prim}}.$$

By (17) and Part(2) of Proposition 48,

$$(18) \quad \alpha(fg) = \alpha(f)\alpha(g)\alpha(f_{\text{prim}}g_{\text{prim}}).$$

Since f_{prim} and g_{prim} are primitive, by Gauss's lemma version 1, $f_{\text{prim}}g_{\text{prim}}$ is primitive. It means that

$$(19) \quad \alpha(f_{\text{prim}}g_{\text{prim}}) = 1.$$

By (18) and (19), we deduce that

$$\alpha(fg) = \alpha(f)\alpha(g).$$

This completes the proof. $\square$

Lemma 51 (Gauss's lemma, version 3). *Suppose $f \in \mathbb{Z}[x] \setminus \{0\}$ and $f(x) = g_1(x)g_2(x)$ for some $g_1, g_2 \in \mathbb{Q}[x]$. Then there exist $c_1, c_2 \in \mathbb{Q}$ such that*

$$(1) \ c_1 c_2 = 1.$$

$$(2) \ c_1 g_1(x), c_2 g_2(x) \in \mathbb{Z}[x]; \text{ in particular, } f(x) = (c_1 g_1(x))(c_2 g_2(x)) \text{ and } \deg(c_i g_i) = \deg g_i.$$

Proof. Since $g_i(x) \in \mathbb{Q}[x]$, there exists $a_i \in \mathbb{Z}^+$ such that

$$\tilde{g}_i(x) := a_i g_i(x) \in \mathbb{Z}[x].$$

Note that

$$(20) \quad a_1 a_2 f(x) = (a_1 g_1(x))(a_2 g_2(x)) = \tilde{g}_1(x) \tilde{g}_2(x).$$

Comparing the contents of both sides of the equation given in (20), it follows that

$$(21) \quad \alpha(\underbrace{a_1 a_2}_{\in \mathbb{Z}^+} f) = \alpha(\tilde{g}_1 \tilde{g}_2).$$

By Part(2) of Proposition 48, the left hand side of the equation in (21) equals $a_1 a_2 \alpha(f)$. By Gauss's lemma, version 2, the right hand side of the equation in (21) equals $\alpha(\tilde{g}_1) \alpha(\tilde{g}_2)$. Altogether, we deduce

$$(22) \quad a_1 a_2 \alpha(f) = \alpha(\tilde{g}_1) \alpha(\tilde{g}_2).$$

On the other hand, by Part(1) of Proposition 48, we have

$$\tilde{g}_i(x) = \alpha(\tilde{g}_i) \tilde{g}_{i,\text{prim}}.$$

Hence, by (20), it follows

$$(23) \quad \begin{aligned} a_1 a_2 f(x) &= \alpha(\tilde{g}_1) \alpha(\tilde{g}_2) \tilde{g}_{1,\text{prim}}(x) \tilde{g}_{2,\text{prim}}(x) \\ &= a_1 a_2 \alpha(f) \tilde{g}_{1,\text{prim}}(x) \tilde{g}_{2,\text{prim}}(x). \end{aligned} \quad (\text{by (22)})$$

Thus, by (23),

$$(24) \quad f(x) = (\alpha(f) \tilde{g}_{1,\text{prim}}(x)) (\tilde{g}_{2,\text{prim}}(x)).$$

Note that $\alpha(f) \tilde{g}_{1,\text{prim}}(x)$ and $\tilde{g}_{2,\text{prim}}(x)$ are polynomials in $\mathbb{Z}[x]$. Hence, (24) gives us a factorization of f over $\mathbb{Z}$. Next, we show that these factors are the same as g_i 's up to multiplication by a rational number. Note that

$$(25) \quad \tilde{g}_{i,\text{prim}}(x) = \alpha(\tilde{g}_i)^{-1} \tilde{g}_i(x) = \underbrace{(\alpha(\tilde{g}_i)^{-1} a_i)}_{\in \mathbb{Q}} g_i(x).$$

Let $c_2 := \alpha(\tilde{g}_2)^{-1} a_2 \in \mathbb{Q}$ and $c_1 := \alpha(f) \alpha(\tilde{g}_1)^{-1} a_1 \in \mathbb{Q}$. Then, by (24), it follows that

$$(26) \quad \begin{aligned} f(x) &= (c_1 g_1(x)) (c_2 g_2(x)) \quad \text{and} \\ c_1 g_1(x) &= \alpha(f) \tilde{g}_{1,\text{prim}}(x) \in \mathbb{Z}[x], \\ c_2 g_2(x) &= \tilde{g}_{2,\text{prim}}(x) \in \mathbb{Z}[x]. \end{aligned}$$

Using (26) and $f(x) = g_1(x) g_2(x)$, we deduce that

$$c_1 c_2 = 1,$$

which completes the proof. $\square$

Corollary 52. *Suppose $f \in \mathbb{Z}[x] \setminus \{0\}$ and $f(x) = g_1(x) \cdots g_n(x)$ for some $g_i \in \mathbb{Q}[x]$. Then there exist $c_i \in \mathbb{Q}$ such that*

$$c_1 \cdots c_n = 1 \quad \text{and} \quad c_i g_i(x) \in \mathbb{Z}[x] \quad \text{for all } i.$$

In particular, $f(x) = (c_1 g_1(x)) \cdots (c_n g_n(x))$ is a factorization of f over $\mathbb{Z}$ and $\deg(c_i g_i) = \deg g_i$.

Proof. (We did not go over the proof of this corollary. I do not expect you to know the proof, but we will be using the statement later. So, you should make sure to understand the claim.) We proceed by induction on n . The case of $n = 2$ follows from Gauss's lemma, version 3. Next, we prove the induction step. Suppose

$$f(x) = g_1(x) \cdots g_{n+1}(x).$$

Let $h(x) := g_1(x) \cdots g_n(x) \in \mathbb{Q}[x]$. Then

$$f(x) = h(x)g_{n+1}(x).$$

Therefore, by Gauss's lemma version 3, there exist $c_{n+1} \in \mathbb{Q}^\times$ such that

$$(27) \quad c_{n+1}g_{n+1}(x) \in \mathbb{Z}[x] \quad \text{and} \quad c_{n+1}^{-1}h(x) \in \mathbb{Z}[x].$$

Note that $c_{n+1}^{-1}h(x) = (c_{n+1}^{-1}g_1(x)) \cdot g_2(x) \cdots g_n(x)$ is in $\mathbb{Z}[x]$. Therefore, by the induction hypothesis, there exist $c'_1, \dots, c'_n \in \mathbb{Q}$ such that

$$c'_1 \cdots c'_n = 1 \quad \text{and} \quad c'_1(c_{n+1}^{-1}g_1(x)), c'_2g_2(x), \dots, c'_ng_n(x) \in \mathbb{Z}[x].$$

Let $c_1 := c'_1c_{n+1}^{-1}$, $c'_2 := c_2, \dots, c_n := c'_n$. Then

$$c_1 \cdot c_2 \cdots c_n \cdot c_{n+1} = c'_1 \cdots c'_n = 1$$

and

$$c_i g_i(x) \in \mathbb{Z}[x],$$

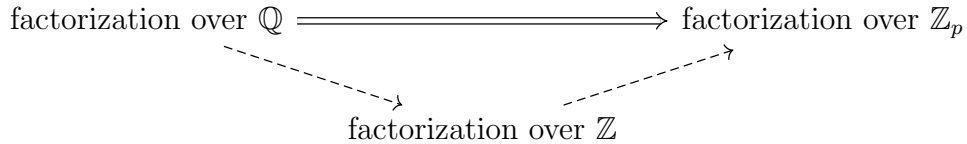
which completes the proof. $\square$

Theorem 53 (Mod- p irreducibility criterion). *Suppose $f \in \mathbb{Z}[x]$ is monic. If f is irreducible in $\mathbb{Z}_p[x]$ for some prime p , then f is irreducible in $\mathbb{Q}[x]$.*

Proof. As we have explained earlier, we prove the contrapositive of this statement:

If f is not irreducible over $\mathbb{Q}$, then f is not irreducible over $\mathbb{Z}_p$.

We may assume that $\deg f \geq 1$. Since $\mathbb{Q}$ and $\mathbb{Z}_p$ are fields, not being irreducible is equivalent to having a factorization into polynomials of positive degree. We will be using a factorization over $\mathbb{Z}$ to connect these two drastically different fields:



Since f is not irreducible over $\mathbb{Q}$ and $\deg f > 0$, there exist $g_1, g_2 \in \mathbb{Q}[x]$ such that $f(x) = g_1(x)g_2(x)$ and $\deg g_i > 0$. By Gauss's lemma version 3, there exists $c_i \in \mathbb{Q}$ such that

$$f(x) = (c_1g_1(x))(c_2g_2(x)) \quad \text{and} \quad h_i(x) := c_i g_i(x) \in \mathbb{Z}[x].$$

Note that $\deg h_i = \deg g_i > 0$. Since $f(x) = h_1(x)h_2(x)$, we deduce that $c_p(f) = c_p(h_1)c_p(h_2)$ where

$$c_p: \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x], \quad c_p\left(\sum_{i=0}^n a_i x^i\right) = \sum_{i=0}^n [a_i]_p x^i$$

is the residue map modulo p . This means we obtained a factorization of f over $\mathbb{Z}_p$. It is remained to argue why $\deg c_p(h_i) > 0$. Note that degree of a polynomial $h \in \mathbb{Z}[x]$ modulo p might be smaller than the degree of h . For instance: $\deg(c_2(2x+1)) = 0 < \deg(2x+1)$. When does this happen? Yes. It happens exactly when p divides the leading coefficient of h . So, we must examine the leading coefficient of h_i . Since $f = h_1h_2$ and $\mathbb{Z}$ is an integral domain, $\ell(f) = \ell(h_1)\ell(h_2)$. As

f is monic, $\ell(h_1)\ell(h_2) = 1$. Therefore, $\ell(h_i) = \pm 1$. Therefore, p does not divide $\ell(h_i)$. Thus, $\deg c_p(h_i) = \deg h_i > 0$. This completes the proof. $\square$

Example 10. Using the fact that $x^p - x + a$ is irreducible in $\mathbb{Z}_p[x]$ if $a \in \mathbb{Z}_p^*$, show that

$$f(x) := x^7 - 14x^5 - 21x^2 - 8x + 9$$

is irreducible in $\mathbb{Q}[x]$.

Proof. Note that f modulo 7 is $x^7 - x + 2$ which is irreducible in $\mathbb{Z}_7[x]$ based on the mentioned theorem. Using the mod- p irreducibility criterion, it follows that f is irreducible in $\mathbb{Q}[x]$. $\square$

Another useful irreducibility criterion is the following.

Theorem 54 (Eisenstein's irreducibility criterion). *Suppose p is prime,*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x],$$

and

$$p \nmid a_n, p \mid a_{n-1}, \dots, p \mid a_0, p^2 \nmid a_0.$$

Then f is irreducible in $\mathbb{Q}[x]$.

Proof. Suppose to the contrary that f is not irreducible in $\mathbb{Q}[x]$. Since $\deg f > 0$ and $\mathbb{Q}$ is a field, not being irreducible implies that f can be written as a product of two polynomials of positive degree: say $f(x) = g_1(x)g_2(x)$ for some $g_1, g_2 \in \mathbb{Q}[x]$ and $\deg g_i > 0$. By Gauss's lemma version 3, there exist $c_1, c_2 \in \mathbb{Q}$ such that

$$f(x) = (c_1 g_1(x))(c_2 g_2(x)) \quad \text{and} \quad h_i(x) := c_i g_i(x) \in \mathbb{Z}[x].$$

Looking at $f(x) = h_1(x)h_2(x)$ modulo p , we deduce that

$$[a_n]_p x^n = c_p(h_1) c_p(h_2).$$

We will show that every polynomial in $\mathbb{Z}_p[x]$ can be written as a product of irreducibles in a unique way (we say $\mathbb{Z}_p[x]$ is a **Unique Factorization Domain (UFD)**). Since x is irreducible, we deduce that the irreducible factors of $c_p(h_i)$ is x . This means $c_p(h_i)$ is a constant times a power of x . In particular, the constant term of $c_p(h_i)$ is zero. Therefore, the constant term of h_i is a multiple of p . Note that the constant term of h_i is $h_i(0)$. Thus,

$$p \mid h_1(0) \quad \text{and} \quad p \mid h_2(0).$$

This implies that

$$p^2 \mid h_1(0)h_2(0) \quad \text{which implies} \quad p^2 \mid f(0).$$

Hence, $p^2 \mid a_0$ which is a contradiction. This completes the proof. $\square$

Example 11. Is $f(x) := 3x^4 - 30x^3 + 20x^2 - 10x + 20$ irreducible in $\mathbb{Q}[x]$?

When you are asked to prove that a polynomial $f \in F[x]$ is irreducible, I suggest going through the following steps:

- (1) If $\deg f = 2$ or 3 over a field F , use the *degree 2 or 3 irreducibility criterion* and reduce the problem to determining whether f has a zero in F .
- (2) If $\deg f > 3$ and $f \in \mathbb{Z}[x]$, try using the *Eisenstein irreducibility criterion*. Examine the prime factors of the constant term, choose those whose squares do not divide the constant term, and check whether the remaining conditions of Eisenstein's criterion are satisfied.
- (3) If the degree is a prime p , check whether $c_p(f)$ is of the form $x^p - x + a$ with $a \in \mathbb{Z}_p^\times$. In this case, use *mod- p irreducibility criterion*.

Solution. Since $\deg f > 3$, we cannot use the degree 2 or 3 irreducibility criterion. So, we try using Eisenstein's irreducibility criterion. Examining the constant term, we see that the only prime factors of 20 are 2 or 5. Since $2^2 | 20$, $p = 2$ is not suitable for applying Eisenstein's irreducibility criterion. We will check that $p = 5$ satisfies the conditions:

$$5 \nmid 3, 5 | 30, 5 | 20, 5 | 10, 5 | 20, 5^2 \nmid 20.$$

Therefore, by Eisenstein's criterion, f is irreducible in $\mathbb{Q}[x]$. $\square$

The following is a non-trivial application of Eisenstein's irreducibility criterion:

Problem. Suppose p is prime. Prove that

$$f(x) := x^{p-1} + x^{p-2} + \cdots + 1$$

is irreducible in $\mathbb{Q}[x]$.

Proof. Recall that $f(x) = \frac{x^p - 1}{x - 1}$. Hence,

$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p-1}{1}.$$

While studying the Frobenius homomorphism, we discussed that

$$\text{for all } 1 \leq i \leq p-1, \quad p \mid \binom{p}{i}.$$

We also note that $p^2 \nmid \binom{p}{1}$. Therefore, by Eisenstein's irreducibility criterion, $f(x+1)$ is irreducible in $\mathbb{Q}[x]$. If $f(x)$ is not irreducible in $\mathbb{Q}[x]$, then $f(x) = g(x)h(x)$ with $g, h \in \mathbb{Q}[x]$ and $\deg g, \deg h > 0$. Hence,

$$f(x+1) = g(x+1)h(x+1),$$

which contradicts that $f(x+1)$ is irreducible. $\square$

11. LECTURE 11: IDEAL, IDEALS GENERATED BY A GIVEN SET OF ELEMENTS, PRINCIPAL IDEALS, KERNELS ARE IDEALS, IDEALS OF A FIELD, PID.

Definition 13. Suppose R is a unital commutative ring. We say I is an ideal of R if for all $a, b \in I$, $a + b \in I$ and for every $a \in I$ and $r \in R$, $ra \in I$.

Example 12. (1) $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

(2) R -linear combinations of $x_1, \dots, x_n$ form an ideal of R . This is the smallest ideal of R which contains all x_i 's. So it is called the ideal generated by $x_1, \dots, x_n$ and it is denoted by $\langle x_1, \dots, x_n \rangle$. Note that

$$\langle x \rangle = \{rx \mid r \in R\}.$$

This should not be confused by the cyclic group generated by x . From the context, you should realize if this notation refers to the ideal generated by x or the cyclic subgroup generated by x . The ideal $\langle x \rangle$ is called the *principal* ideal generated by x .

(3) If $f: R_1 \rightarrow R_2$ is a group homomorphism, then $\ker f$ is an ideal of R_1 .

Proof. (1) Note that $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$, so it suffices to check that for every $x \in \mathbb{Z}$ and $y \in n\mathbb{Z}$, $xy \in n\mathbb{Z}$. This is clear as $y = nk$ for some $k \in \mathbb{Z}$, which implies $xy = n(xk) \in n\mathbb{Z}$.

Note that every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$. Hence, all ideals of $\mathbb{Z}$ are of this form.

(2) For an R -linear combination $c_1x_1 + \cdots + c_nx_n$ and $c \in R$, we have

$$c(c_1x_1 + \cdots + c_nx_n) = (cc_1)x_1 + \cdots + (cc_n)x_n$$

which is again an R -linear combination of x_i 's. Adding two R -linear combinations of x_i 's result in another such element.

Note that $n\mathbb{Z}$ is the principal ideal generated by n . Therefore, by the above remark, every ideal of $\mathbb{Z}$ is principal.

(3) Kernel of a subgroup of $(R_1, +)$, so it suffices to check the multiplication condition for being an ideal. Suppose $x \in \ker f$ and $r_1 \in R_1$. We must show that $r_1x \in \ker f$. Note that

$$f(r_1x) = f(r_1)f(x) = f(r_1) \cdot 0 = 0, \quad \text{and so } r_1x \in \ker f.$$

□

Lemma 55. Suppose R is a unital commutative ring. For every $r \in R$,

$$\langle r \rangle = R \iff r \in R^\times.$$

Hence, R has exactly two (distinct) ideals $\{0\}$ and R if and only if R is a field.

Proof. ($\Rightarrow$) Since $1 \in \langle r \rangle$, there exists $r' \in R$ such that $1 = rr'$, which means $r \in R^\times$.

($\Leftarrow$) For every $x \in R$, $x = r(r^{-1}x) \in \langle r \rangle$. Therefore $\langle r \rangle = R$.

Suppose R is a field and I is a non-zero ideal of R . Then there exists $r \in I$ which is in $R \setminus \{0\} = R^\times$. Then $I \supseteq \langle r \rangle = R$. Hence, $I = R$.

Suppose the only ideals of R are $\{0\}$ and R . Then for every non-zero element r , we have $\langle r \rangle = R$, which implies that $r \in R^\times$. This completes the proof. □

This result plays an important role in understanding *maximal* ideals as we will see later.

Definition 14. An integral domain D is called a Principal Ideal Domain (PID) if every ideal is principal.

Theorem 56. $\mathbb{Z}$ and $F[x]$, where F is a field, are PIDs.

Proof. Suppose I is a non-zero ideal of $F[x]$. Let $f(x) \in I \setminus \{0\}$ be a polynomial with smallest possible degree. We claim that $I = \langle f(x) \rangle$.

Clearly, $\langle f \rangle \subseteq I$. So, we focus on the direction. Suppose $g \in I$. By the long division algorithm, there exists a unique pair of polynomials (q, r) such that

$$g(x) = f(x)q(x) + r(x) \quad \text{and} \quad \deg r < \deg f.$$

Then $r(x) = g(x) - q(x)f(x) \in I$.

What can we deduce based on the following statements:

- (1) $\deg f$ is minimum among the degree of non-zero elements of I ,
- (2) $r \in I$, and
- (3) $\deg r < \deg f$.

That is right! $r = 0$. Therefore, $g(x) = f(x)q(x) \in \langle f \rangle$. This implies that $I \subseteq \langle f \rangle$, which completes the proof. □

12. LECTURE 12: QUOTIENT RING, FUNDAMENTAL THEOREM OF HOMOMORPHISM, EVALUATION MAP REVISITED, ALGEBRAIC ELEMENTS

Lemma 57 (Quotient of a ring by an ideal). Suppose I is an ideal of R .

- (1) For $x+I, y+I \in R/I$, define $(x+I) \cdot (y+I) := xy+I$. Then this operation is well-defined, and $(R/I, +, \cdot)$ is a ring.
- (2) The map $\pi: R \rightarrow R/I$, $\pi(x) := x+I$ is a surjective ring homomorphism. It is called the natural quotient map of R modulo I .
- (3) The kernel of π is I .

Before we prove the above lemma, let's recall from group theory that for a subgroup H ,

$$x_1H = x_2H \iff x_2^{-1}x_1 \in H.$$

In the additive form, we have

$$x_1 + I = x_2 + I \iff x_1 - x_2 \in I.$$

From group theory, we know that R/I is an abelian group with the operation

$$(x + I) + (y + I) := (x + y) + I.$$

So, to prove the above lemma, we may focus only on the multiplication.

Proof of Lemma 57. The important issue is to show that the operation $\cdot$ is well-defined. This means we must prove the following implication:

$$\left. \begin{array}{l} x_1 + I = x_2 + I \\ y_1 + I = y_2 + I \end{array} \right\} \implies x_1y_1 + I = x_2y_2 + I.$$

By the reminder from group theory, we must show

$$\left. \begin{array}{l} x_1 - x_2 \in I \\ y_1 - y_2 \in I \end{array} \right\} \implies x_1y_1 - x_2y_2 \in I.$$

We use an argument similar to Lemma 4, where we discussed congruence arithmetic:

$$\begin{aligned} x_1y_1 - x_2y_2 &= x_1y_1 - x_1y_2 + x_1y_2 - x_2y_2 \\ &= x_1 \underbrace{(y_1 - y_2)}_{\in I} + \underbrace{(x_1 - x_2)}_{\in I} y_2 \\ &\in I. \end{aligned}$$

This shows that $\cdot$ is a well-defined operation on R/I . Since the operations $+$ and $\cdot$ are defined using the coset representatives, algebraic operations in R/I are symbolically the same as the ones in R with an additional *decoration* $+I$. Hence, all algebraic equations in R are also satisfied in R/I . We only check the distribution law. The remaining conditions can be checked by a similar logic.

$$\begin{aligned} (x + I) \cdot ((y + I) + (z + I)) &= (x + I) \cdot ((y + z) + I) \\ &= x(y + z) + I = (xy + xz) + I \\ &= (xy + I) + (xz + I) \\ &= (x + I) \cdot (y + I) + (x + I) \cdot (z + I). \end{aligned}$$

(2) Clearly, π is surjective. For every $x, y \in R$,

$$\begin{aligned} \pi(x) + \pi(y) &= (x + I) + (y + I) = (x + y) + I = \pi(x + y) \\ \pi(x) \cdot \pi(y) &= (x + I) \cdot (y + I) = (xy) + I = \pi(xy). \end{aligned}$$

(3) $x \in \ker \pi \iff \pi(x) = 0 \iff x + I = 0 + I \iff x \in I$. This shows that $\ker \pi = I$. $\square$

Theorem 58 (The fundamental theorem of ring homomorphisms). *Suppose $f: R \rightarrow S$ is a ring homomorphism. Then the following is a ring isomorphism:*

$$\bar{f}: R/\ker f \rightarrow \text{Im}(f), \quad \bar{f}(r + \ker f) := f(r).$$

Proof. From group theory, we know that $\bar{f}$ is a well-defined group isomorphism. So, it suffices to show why $\bar{f}$ preserves the multiplication.

Because of the importance of this result, we recall why $\bar{f}$ is well-defined and injective:

$$r_1 + \ker f = r_2 + \ker f \iff r_1 - r_2 \in \ker f \iff f(r_1 - r_2) = 0 \iff f(r_1) = f(r_2).$$

Clearly $\bar{f}$ is surjective, and so it is a bijection. We check that $\bar{f}$ preserves multiplication:

$$\begin{aligned}\bar{f}((r_1 + \ker f)(r_2 + \ker f)) &= \bar{f}((r_1 r_2) + \ker f) = f(r_1 r_2), \\ \bar{f}(r_1 + \ker f)\bar{f}(r_2 + \ker f) &= f(r_1)f(r_2) = f(r_1 r_2).\end{aligned}$$

□

We may capture the Fundamental Theorem of Homomorphisms via the following diagram:

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \pi \downarrow & & \uparrow \\ R/\ker f & \xrightarrow{\bar{f}} & \text{Im}(f) \end{array}$$

We say this diagram is a commuting diagram. This way we may remember what the definition of $\bar{f}$. Let's how we may apply this result for an evaluation map.

Example 13. Consider the evaluation map at $\sqrt[3]{2}$,

$$e_{\sqrt[3]{2}}: \mathbb{Q}[x] \rightarrow \mathbb{R}.$$

What can we say about the image and the kernel of this ring homomorphism?

Solution. $\ker e_{\sqrt[3]{2}}$ is an ideal of $\mathbb{Q}[x]$. Since $\mathbb{Q}$ is a field, $\mathbb{Q}[x]$ is a PID. Therefore, every ideal of $\mathbb{Q}[x]$ is principal. Thus, there exists a polynomial $m_{\sqrt[3]{2}}$ such that

$$\ker e_{\sqrt[3]{2}} = \langle m_{\sqrt[3]{2}}(x) \rangle.$$

Note that multiplying by the inverse of the leading coefficient of $m_{\sqrt[3]{2}}(x)$ does not change the principal ideal generated by this polynomial. Hence, we may assume that $m_{\sqrt[3]{2}}(x)$ is monic.

Observe that $x^3 - 2$ is in $\ker e_{\sqrt[3]{2}}$. Therefore, $m_{\sqrt[3]{2}}(x)$ divides $x^3 - 2$. Since $x^3 - 2$ has no zero in $\mathbb{Q}$, by the degree 2 or 3 irreducibility criterion $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$. Therefore, it cannot be written as a product of positive degree polynomials. Since $m_{\sqrt[3]{2}}(x)$ divides $x^3 - 2$, it follows that $m_{\sqrt[3]{2}}(x) = c(x^3 - 2)$ for some $c \in \mathbb{Q}^\times$. Because $m_{\sqrt[3]{2}}(x)$ is monic,

$$m_{\sqrt[3]{2}}(x) = x^3 - 2.$$

By the fundamental theorem of homomorphisms,

$$\mathbb{Q}[x]/\ker e_{\sqrt[3]{2}} \simeq \text{Im } e_{\sqrt[3]{2}}.$$

Thus

$$\mathbb{Q}[x]/\langle x^3 - 2 \rangle \simeq \text{Im}(e_{\sqrt[3]{2}}).$$

For every $f \in \mathbb{Q}[x]$, by the long division, there exists a unique pair (q, r) such that

$$f(x) = q(x)(x^3 - 2) + r(x) \quad \text{and} \quad \deg r < \deg(x^3 - 2).$$

Thus $f(x) - r(x) \in \langle x^3 - 2 \rangle$ and $r(x) = c_0 + c_1x + c_2x^2$ for some $c_i \in \mathbb{Q}$. Hence,

$$f(x) + \langle x^3 - 2 \rangle = c_0 + c_1x + c_2x^2 + \langle x^3 - 2 \rangle,$$

for unique $c_0, c_1, c_2 \in \mathbb{Q}$. This implies

$$(28) \quad \mathbb{Q}[x]/\langle x^3 - 2 \rangle = \{c_0 + c_1x + c_2x^2 + \langle x^3 - 2 \rangle \mid c_0, c_1, c_2 \in \mathbb{Q}\},$$

and because of the uniqueness, we deduce that

$$1 + \langle x^3 - 2 \rangle, x + \langle x^3 - 2 \rangle, x^2 + \langle x^3 - 2 \rangle$$

form a $\mathbb{Q}$ -basis of $\mathbb{Q}[x]/\langle x^3 - 2 \rangle$.

The fundamental theorem of homomorphism implies that

$$\bar{e}_{\sqrt[3]{2}}(f(x) + \langle x^3 - 2 \rangle) := f(\sqrt[3]{2})$$

is an isomorphism between $\mathbb{Q}[x]/\langle x^3 - 2 \rangle$ and $\text{Im}(e_{\sqrt[3]{2}})$. By (28), we deduce that

$$\text{Im}(e_{\sqrt[3]{2}}) = \{c_0 + c_1\sqrt[3]{2} + c_2\sqrt[3]{2}^2 \mid c_0, c_1, c_2 \in \mathbb{Q}\},$$

and $1, \sqrt[3]{2}$, and $\sqrt[3]{2}^2$ are linearly independent over $\mathbb{Q}$. Later, we will show that the image is a field. $\square$

Definition 15. Suppose $\alpha \in \mathbb{C}$. We say α is *algebraic* (over $\mathbb{Q}$) if α is a zero of a non-zero polynomial in $\mathbb{Q}[x]$. Otherwise, we say α is *transcendental* (over $\mathbb{Q}$).

We may define similar concepts over an arbitrary field F instead of $\mathbb{Q}$.

13. LECTURE 13: MINIMAL POLYNOMIAL, CORRESPONDENCE THEOREM, MAXIMAL IDEALS, IRREDUCIBLE ELEMENTS IN A PID AND MAXIMAL IDEALS.

Recall that $e_\alpha: \mathbb{Q}[x] \rightarrow \mathbb{C}$, $e_\alpha(f) := f(\alpha)$ is a ring homomorphism and its kernel is not zero if and only if α is algebraic. There are many transcendental elements, for instance π , e , etc. It is, however, not easy to prove a given number is transcendental. In this course, we focus on algebraic elements.

The image of e_α is

$$\{f(\alpha) \mid f \in \mathbb{Q}[x]\}.$$

It is denoted by $\mathbb{Q}[\alpha]$. It is the smallest subring of $\mathbb{C}$ which contains $\mathbb{Q}$ and α .

Our goal is study the kernel and the image of e_α .

Proposition 59 (Minimal polynomial). *For every algebraic element $\alpha \in \mathbb{C}$, there exists a unique monic polynomial $m_\alpha \in \mathbb{Q}[x]$ with the following properties:*

- (1) $m_\alpha(\alpha) = 0$.
- (2) If $f \in \mathbb{Q}[x]$ and $f(\alpha) = 0$, then $m_\alpha(x) \mid f(x)$ in $\mathbb{Q}[x]$.
- (3) If $f \in \mathbb{Q}[x] \setminus \{0\}$ and $f(\alpha) = 0$, then $\deg f \geq \deg m_\alpha$.
- (4) $\ker e_\alpha = \langle m_\alpha \rangle$.
- (5) $m_\alpha(x)$ is irreducible in $\mathbb{Q}[x]$.
- (6) If $p(x) \in \mathbb{Q}[x]$ is monic and irreducible and $p(\alpha) = 0$, then $p(x) = m_\alpha(x)$.

Proof. Let $e_\alpha: \mathbb{Q}[x] \rightarrow \mathbb{C}$ be the evaluation at α map. Then $\ker e_\alpha$ is an ideal of $\mathbb{Q}[x]$. Since $\mathbb{Q}$ is a field, $\mathbb{Q}[x]$ is a PID. Therefore, $\ker e_\alpha$ is a principal ideal. Since α is algebraic, $\ker e_\alpha$ is non-zero. After multiplying by the inverse of the leading coefficient of its generator, we obtain a monic polynomial m_α which generates $\ker e_\alpha$.

Therefore, for $f \in \mathbb{Q}[x]$, α is a zero of f if and only if $f \in \ker e_\alpha$ if and only if $m_\alpha(x) \mid f(x)$ in $\mathbb{Q}[x]$.

If $f \in \mathbb{Q}[x] \setminus \{0\}$ and $f(\alpha) = 0$, then $f(x) = m_\alpha(x)q(x)$ for some non-zero polynomial $q \in \mathbb{Q}[x]$. Comparing the degrees of both sides, we deduce

$$\deg f = \deg m_\alpha + \deg q \geq \deg m_\alpha.$$

Suppose to the contrary that $m_\alpha(x)$ is not irreducible in $\mathbb{Q}[x]$. Since $\mathbb{Q}$ is field and $m_\alpha(x)$ is a positive degree polynomial, there exist $g_1, g_2 \in \mathbb{Q}[x]$ such that $m_\alpha(x) = g_1(x)g_2(x)$. Evaluating both sides at α , we deduce

$$g_1(\alpha)g_2(\alpha) = m_\alpha(\alpha) = 0.$$

Since $\mathbb{C}$ is a field, it has no zero-divisors. Hence, either $g_1(\alpha) = 0$ or $g_2(\alpha) = 0$. Thus, either $\deg g_1 \geq \deg m_\alpha$ or $\deg g_2 \geq \deg m_\alpha$. This is a contradiction as $\deg m_\alpha = \deg g_1 + \deg g_2$.

Since α is a zero of p and $p \in \mathbb{Q}[x]$, $m_\alpha(x)$ divides $p(x)$ in $\mathbb{Q}[x]$. This means $p(x) = m_\alpha(x)q(x)$ for some $q \in \mathbb{Q}[x]$. Since p is irreducible in $\mathbb{Q}[x]$, $p(x) = m_\alpha(x)q(x)$ implies that $q(x) = c$ is a non-zero constant polynomial. So, $p(x) = cm_\alpha(x)$. Comparing the leading coefficients of both sides, it follows that $\ell(p) = c\ell(m_\alpha)$. Since p and m_α are monic, $\ell(p) = \ell(m_\alpha) = 1$. Therefore, $c = 1$, which implies $p(x) = m_\alpha(x)$. This completes the proof. $\square$

Example 14. Find the minimal polynomial of $\sqrt[n]{2}$ over $\mathbb{Q}$.

Solution. Note that $\sqrt[n]{2}$ is a zero of $x^n - 2 \in \mathbb{Q}[x]$. Observe that $2 \nmid 1$, $2 \mid 0$, $2 \mid 2$, and $2^2 \nmid 2$. Therefore, by Eisenstein's irreducibility criterion, $x^n - 2$ is irreducible in $\mathbb{Q}[x]$. Since $x^n - 2$ is monic, irreducible, and $\sqrt[n]{2}$ is a zero of $x^n - 2$, by Part(6) of Proposition 59, $m_{\sqrt[n]{2}}(x) = x^n - 2$. $\square$

Example 15. Suppose $\alpha \in \mathbb{C}$ is a zero of $f(x) := x^6 - 14x^3 + 98x - 28$. Find $m_\alpha(x)$.

Solution. Note that $7 \nmid 1$, $7 \mid 14$, $7 \mid 98$, $7 \mid 28$, and $7^2 \nmid 28$. Therefore, by Eisenstein's irreducibility criterion, f is irreducible. f is monic, irreducible in $\mathbb{Q}[x]$, and α is a zero of f . Thus by Part(6) of Proposition 59, $m_\alpha(x) = f(x)$. $\square$

Now that we have a relatively good understanding of the kernel of e_α , we study its image. Let's recall that the image of e_α is denoted by $\mathbb{Q}[\alpha]$.

Lemma 60. For an algebraic element $\alpha \in \mathbb{C}$,

$$\dim_{\mathbb{Q}} \mathbb{Q}[\alpha] = \deg m_\alpha,$$

and $\{1, \alpha, \dots, \alpha^{d-1}\}$ is a $\mathbb{Q}$ -basis of $\mathbb{Q}[\alpha]$ where $d := \deg m_\alpha$.

Proof. We must show two statements: (1) every element of $\mathbb{Q}[\alpha]$ is a $\mathbb{Q}$ -linear combination of $1, \alpha, \dots, \alpha^{d-1}$. (2) $1, \alpha, \dots, \alpha^{d-1}$ are $\mathbb{Q}$ -linearly independent.

Every element of $\mathbb{Q}[\alpha]$ is of the form $f(\alpha)$ for some $f \in \mathbb{Q}[x]$. By the long division algorithm, there exists a unique pair (q, r) of polynomials in $\mathbb{Q}[x]$ satisfying the following:

$$(29) \quad f(x) = m_\alpha(x)q(x) + r(x) \quad \text{and} \quad \deg r < \deg m_\alpha.$$

Hence, $r(x) = c_0 + c_1x + \dots + c_{d-1}x^{d-1}$ for some $c_i \in \mathbb{Q}$. By evaluating both sides of (29) at α , it follows that

$$f(\alpha) = \underbrace{m_\alpha(\alpha)}_{=0} q(\alpha) + r(\alpha) = c_0 + c_1\alpha + \dots + c_{d-1}\alpha^{d-1}.$$

Hence, every element of $\mathbb{Q}[\alpha]$ is a $\mathbb{Q}$ -linear combination of $1, \alpha, \dots, \alpha^{d-1}$.

Next, we show why they are $\mathbb{Q}$ -linearly independent. Suppose a $\mathbb{Q}$ -linear combination of them is zero:

$$c_0 + c_1\alpha + \dots + c_{d-1}\alpha^{d-1} = 0.$$

This implies the α is a zero of $f(x) := c_0 + c_1x + \dots + c_{d-1}x^{d-1}$. By Proposition 59, degree of a non-zero polynomial having α as a zero is at least $d = \deg m_\alpha$. Since $\deg f < d$ and α is a zero of f , we deduce that $f(x) = 0$. This means

$$c_0 = c_1 = \dots = c_{d-1} = 0.$$

This completes the proof. $\square$

One can also use the following Lemma:

Lemma 61. Suppose F is a field and $f \in F[x]$ is of degree n . Then $\dim_F F[x]/\langle f(x) \rangle = \deg f$. In fact,

$$\{1 + \langle f \rangle, x + \langle f \rangle, \dots, x^{\deg f - 1} + \langle f \rangle\}$$

is an F -basis of $F[x]/\langle f \rangle$.

By the fundamental theorem of homomorphisms,

$$\mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/\langle m_\alpha \rangle.$$

We wish to show that $\mathbb{Q}[\alpha]$ is a field. So, we must know when R/I is a field?

For a ring R , let $\text{Ideal}(R)$ be the set of its ideals. Recall that for a unital commutative ring R , $\text{Ideal}(R)$ has exactly two distinct elements $\{0\}$ and R if and only if R is a field. So, R/I is a field if and only if $\text{Ideal}(R/I)$ has exactly two elements.

Theorem 62 (Correspondence theorem). *Suppose I is an ideal of R . Then the following maps are bijections:*

$$\begin{aligned} \{J \in \text{Ideal}(R) \mid I \subseteq J\} &\rightarrow \text{Ideal}(R/I), & J &\mapsto J/I, \\ \text{Ideal}(R/I) &\rightarrow \{J \in \text{Ideal}(R) \mid I \subseteq J\}, & \bar{J} &\mapsto \{x \in R \mid x + I \in \bar{J}\}. \end{aligned}$$

Proof. **Step 1.** The above maps give us ideals.

Since $I \subseteq J$, J/I makes sense as a subset of R/I . For every $x, x' \in I$ and $r \in R$, we have

$$(x + I) + (r + I) \cdot (x' + I) = (x + rx') + I \in J/I \quad \text{since} \quad x + rx' \in J.$$

This shows J/I is an ideal of R/I .

If $x + I, x' + I \in \bar{J}$ and $r \in R$, then

$$(x + I) + (r + I) \cdot (x' + I) = (x + rx') + I \in \bar{J}.$$

So, $\{x \in R \mid x + I \in \bar{J}\}$ is an ideal of R .

Step 2. $\{x \in R \mid x + I \in \bar{J}\} \supseteq I$.

For every $x' \in I$, $x' + I = 0 + I \in \bar{J}$. Hence, $x \in \{x \in R \mid x + I \in \bar{J}\}$.

Step 3. These maps are inverse of each other.

We must show

$$\{x \in R \mid x + I \in J/I\} = J \quad \text{and} \quad \{x \in R \mid x + I \in \bar{J}\}/I = \bar{J}.$$

For $x \in J$, clearly $x + I \in J/I$. Conversely, if $x + I \in J/I$, then there exists $x' \in J$ such that $x + I = x' + I$. Hence, $x - x' \in I$. Since $I \subseteq J$, it follows that $x - x' \in J$. We deduce that $x \in J$ as x' is also in J .

The second equality is clear. □

Corollary 63. *Suppose R is a unital commutative ring. Then R/I is a field if and only if*

$$\{J \in \text{Ideal}(R) \mid I \subseteq J \subseteq R\}$$

has exactly two distinct elements I and R .

Proof. R/I is a field if and only if $|\text{Ideal}(R/I)| = 2$. By the correspondence theorem, we have $|\text{Ideal}(R/I)| = 2$ if and only if $|\{J \in \text{Ideal}(R) \mid I \subseteq J \subseteq R\}| = 2$. Note that I and R are in this set, and if they are equal, then this set only one element which is R . This completes the proof. □

Definition 16. We say an ideal I of R is maximal if (1) I is proper; that means $I \neq R$ and (2) if $I \subseteq J \subseteq R$ and J is an ideal of R , then either $J = I$ or $J = R$.

Altogether, we have:

Proposition 64. *Suppose R is a unital commutative ring and I is an ideal of R . Then R/I is a field if and only if I is a maximal ideal.*

Example 16. Suppose R is a unital commutative ring. Show that $\{0\}$ is a maximal ideal if and only if R is a field.

Solution. Note that $\{0\}$ is a maximal ideal if and only if $\text{Ideal}(R)$ has exactly two ideals, $\{0\}$ and R . As we have seen before, this is equivalent to R being a field. $\square$

Example 17. Find all the maximal ideals of $\mathbb{Z}$.

Solution. Recall that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}^{\geq 0}$. By the previous example, we know that $n \neq 0$ as $\mathbb{Z}$ is not a field. We know that $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ which is a field if and only if n is prime. Therefore, the set of maximal ideals of $\mathbb{Z}$ are of the form $p\mathbb{Z}$ where p is a prime number. $\square$

Next, we want to understand maximal ideals of all PIDs. Our motivation is to show $\langle m_\alpha \rangle$ is a maximal ideal of $\mathbb{Q}[x]$, and deduce that $\mathbb{Q}[\alpha]$ is a field.

Proposition 65. *Suppose D is a PID. Then $\langle a \rangle$ is maximal if and only if a is irreducible.*

(Started its proof. It will be finished in the next lecture.)

14. LECTURE 14: MAXIMAL IDEALS OF PIDS AND IRREDUCIBLE ELEMENTS. IMAGE OF THE EVALUATION MAP AT AN ALGEBRAIC ELEMENT. PRIME IDEALS. PRIME ELEMENTS. CONNECTION BETWEEN PRIME AND IRREDUCIBLE

One of Kummer's key conceptual insights is that many arithmetic phenomena are best understood by studying ideals rather than individual elements. In this spirit, we aim to analyze properties of elements of a ring through the principal ideals they generate.

Lemma 66. *Suppose D is an integral domain. Then $\langle a \rangle = \langle b \rangle$ if and only if $a = bu$ for some unit u .*

Proof. Since $\langle a \rangle = \langle b \rangle$, $a = bx$ and $b = ay$ for some $x, y \in D$. Hence, $a = (ay)x$. Since D is an integral domain, we may apply the cancellation law, which implies that either $a = 0$ or $1 = yx$.

If $a = 0$, then $b = (a)(y) = (0)(y) = 0$, so $a = b = 0$.

If $a \neq 0$, then $xy = 1$, which implies $x, y \in D^\times$. Hence, $a = bx$ with $x \in D^\times$. $\square$

Proposition 67. *Suppose D is a PID and not a field. Then $\langle a \rangle$ is maximal if and only if a is irreducible.*

Proof. $(\Rightarrow)$ We must show that a satisfies three properties: (1) $a \neq 0$, (2) $a \notin D^\times$, (3) $a = bc$ implies $b \in D^\times$ or $c \in D^\times$.

If $a = 0$, then $\{0\}$ is a maximal ideal, which implies D is a field. This is a contradiction.

If $a \in D^\times$, then $\langle a \rangle = D$ which is not a maximal ideal. This is again a contradiction.

If $a = bc$, then $a \in \langle b \rangle$, which implies $\langle a \rangle \subseteq \langle b \rangle$. Since $\langle a \rangle$ is a maximal ideal, we have that either $\langle b \rangle = \langle a \rangle$ or $\langle b \rangle = D$.

If $\langle b \rangle = \langle a \rangle$, then $a = bu$ for some $u \in D^\times$. Since $a = bc$ and $b \neq 0$, by the cancellation law, $c = u \in D^\times$.

If $\langle b \rangle = D$, then $b \in D^\times$. We have proved that a satisfies all the desired properties.

$(\Leftarrow)$ We must show that (1) $\langle a \rangle$ is proper, and (2) If J is an ideal of D and $\langle a \rangle \subseteq J$, then either $J = \langle a \rangle$ or $J = D$.

Since a is irreducible, $a \notin D^\times$, which implies that $\langle a \rangle \neq D$.

Suppose J is an ideal of D and $\langle a \rangle \subseteq J$. Since D is a PID, $J = \langle b \rangle$ for some $b \in D$.

Since $\langle a \rangle \subseteq \langle b \rangle$, $a = bx$ for some $x \in D$. Since a is irreducible, we deduce that either b is a unit or x is a unit.

If b is a unit, then $J = \langle b \rangle = D$.

If x is a unit, then $\langle a \rangle = \langle b \rangle = J$ as $a = bx$ and $x \in D^\times$. This completes the proof. $\square$

Corollary 68. *Suppose α is algebraic. Then $\mathbb{Q}[\alpha]$ is a field.*

Proof. By the fundamental theorem of homomorphisms, $\mathbb{Q}[x]/\ker e_\alpha \simeq \text{Im } e_\alpha$. We have proved that $\ker e_\alpha = \langle m_\alpha \rangle$ and m_α is irreducible in $\mathbb{Q}[x]$. Since $\mathbb{Q}$ is a field, $\mathbb{Q}[x]$ is a PID (and it is not a field). Therefore, $\langle m_\alpha \rangle$ is a maximal ideal of $\mathbb{Q}[x]$. Hence,

$$\mathbb{Q}[\alpha] = \text{Im } e_\alpha \simeq \mathbb{Q}[x]/\langle m_\alpha \rangle$$

is a field. □

Altogether, we obtain the following important theorem. We proved this theorem for $F = \mathbb{Q}$, but our argument works equally well in this more general setting.

Theorem 69. *Suppose F is a subfield of a field E , and $\alpha \in E$ is algebraic over F . Then*

- (1) *There exists a unique monic polynomial $m_{\alpha;F}(x) \in F[x]$ with the following properties:*
 - (a) *α is a zero of $f(x) \in F[x]$ if and only if $m_{\alpha;F}(x) \mid f(x)$ in $F[x]$.*
 - (b) *$m_{\alpha;F}(x)$ is irreducible in $F[x]$.*
 - (c) *If $p(x) \in F[x]$ is irreducible, monic, and α is a zero of p , then $p(x) = m_{\alpha;F}(x)$.*
- (2) *The image of e_α is denoted by $F[\alpha]$. $\{1, \alpha, \dots, \alpha^{d-1}\}$ is an F -basis of $F[\alpha]$ where $d := \deg m_{\alpha;F}$. In particular,*

$$F[\alpha] = \{c_0 + c_1\alpha + \dots + c_{d-1}\alpha^{d-1} \mid c_i \in F\},$$

and $\dim_F F[\alpha] = \deg m_{\alpha;F}$.

- (3) *$F[\alpha] \simeq F[x]/\langle m_{\alpha;F} \rangle$ and it is a field.*

Next, we investigate when a quotient R/I is an integral domain.

Note that R/I is an integral domain if and only if it is not the trivial ring and it has no zero-divisors. The first condition is equivalent to saying that I is a proper ideal, and the second condition says:

$$(x + I) \cdot (y + I) = 0 + I \iff (x + I = 0 + I \text{ or } y + I = 0 + I).$$

This is equivalent to saying

$$xy \in I \iff x \in I \text{ or } y \in I.$$

This leads us to the definition of a prime ideal.

Definition 17. We say an ideal P of R is prime if

- (1) P is proper and
- (2) $xy \in P$ implies $x \in P$ or $y \in P$.

So, we proved:

Proposition 70. *Suppose R is a unital commutative ring and I is an ideal of R . Then I is a prime ideal if and only if R/I is an integral domain.*

Proof. ($\Rightarrow$) Since I is a prime ideal, it is proper. Hence, R/I is not the trivial ring.

Next, we must show that R/I has no zero-divisors. Suppose $(a + I) \cdot (b + I) = 0$. Then $ab \in I$. Since I is a prime ideal, we have that either $a \in I$ or $b \in I$. This is equivalent to saying

$$a + I = \bar{0} \quad \text{and} \quad b + I = \bar{0}.$$

We may express this argument in mathematical language as follows

$$\begin{aligned} (a + I) \cdot (b + I) = \bar{0} &\Rightarrow ab + I = \bar{0} \\ &\Rightarrow ab \in I \quad (\text{since } I \text{ is prime}) \\ &\Rightarrow a \in I \quad \text{or} \quad b \in I \\ &\Rightarrow a + I = \bar{0} \quad \text{or} \quad b + I = \bar{0}. \end{aligned}$$

($\Leftarrow$) We have already proved. In fact, showing this direction lead us to the definition of a prime ideal. $\square$

Corollary 71. *Suppose R is a unital commutative ring. Then every maximal ideal of R is prime.*

Proof.

$$\begin{aligned} M \text{ maximal ideal of } R &\Rightarrow R/M \text{ is a field} \\ &\Rightarrow R/M \text{ is an integral domain} \\ &\Rightarrow M \text{ is a prime ideal.} \end{aligned}$$

$\square$

Example 18. Suppose R is a unital commutative ring. Show that $\{0\}$ is a prime ideal of R if and only if R is an integral domain.

Proof. $\{0\}$ is a prime ideal if and only if $R/\{0\}$ is an integral domain. Note that $R/\{0\} \simeq R$, and the claim follows. $\square$

Recall that $\{0\}$ is a maximal ideal if and only if R is a field. So, for every integral domain D which is not field, $\{0\}$ is a prime ideal and it is not a maximal ideal.

The above example also shows a subtle point: a prime ideal of $\mathbb{Z}$ is not necessarily of the form $p\mathbb{Z}$ where p is prime! An ideal of $\mathbb{Z}$ is prime if and only if it is either $\{0\}$ or of the form $p\mathbb{Z}$ where p is prime.

When is a principal ideal $\langle a \rangle$ prime?

The ideal $\langle a \rangle$ is prime if and only if $\langle a \rangle \neq R$ and

$$xy \in \langle a \rangle \implies x \in \langle a \rangle \text{ or } y \in \langle a \rangle.$$

We have seen that

$$\langle a \rangle = R \iff a \in R^\times.$$

So, the first condition is that a should not be a unit. The second condition may be rewritten as

$$a|xy \implies a|x \text{ or } a|y.$$

This leads us to the definition of a prime element:

Definition 18. Suppose R is an integral domain. We say $a \in R$ is prime if $a \neq 0$, $a \notin R^\times$ and

$$a|xy \text{ implies } a|x \text{ or } a|y.$$

We have proved:

Lemma 72. *In an integral domain D , a is a prime element if and only if $a \neq 0$ and $\langle a \rangle$ is a prime ideal.*

Proof. ($\Rightarrow$) Since a is prime, then $a \neq 0$ and $a \notin D^\times$. Therefore, $\langle a \rangle \neq D^\times$. Next, we must show

$$bc \in \langle a \rangle \stackrel{?}{\implies} b \in \langle a \rangle \text{ or } c \in \langle a \rangle.$$

Here is the reasoning:

$$\begin{aligned} bc \in \langle a \rangle &\Rightarrow a|bc \quad (\text{since } a \text{ is prime}) \\ &\Rightarrow a|b \text{ or } a|c \\ &\Rightarrow b \in \langle a \rangle \text{ or } c \in \langle a \rangle. \end{aligned}$$

($\Leftarrow$) We have already proved this direction. In fact, this lead us to the definition of a prime element. $\square$

Corollary 73. *Suppose D is a PID. Then a irreducible implies that a is prime.*

Proof. Note that if D is a field, then it has no irreducible elements. So, we may assume that D is not a field. Then

$$\begin{aligned} a \text{ irreducible} &\Rightarrow \langle a \rangle \text{ is maximal as } D \text{ is a PID and not a field} \\ &\Rightarrow \langle a \rangle \text{ is prime and not zero} \\ &\Rightarrow a \text{ is prime.} \end{aligned}$$

□

Note that the above Corollary applied to $D = \mathbb{Z}$ is Euclid's lemma. Let's remark that the classical definition of *prime integers* is equivalent to our definition of irreducible elements. Hence, the above corollary shows for a prime integer p ,

$$p|ab \implies p|a \quad \text{or} \quad p|b.$$

This justifies why there is a consistency with our definitions and the classical arithmetic.

The converse is true for every integral domain.

Lemma 74. *Suppose D is an integral domain and a is prime in D . Then a is irreducible.*

Proof. We must show $a \neq 0$, $a \notin D^\times$, and $a = bc$ implies either $b \in D^\times$ or $c \in D^\times$. Since that a is prime, the first two conditions are automatically satisfied.

$$\begin{aligned} a = bc &\implies a|bc \quad (\text{since } a \text{ is prime}) \\ &\implies a|b \quad \text{or} \quad a|c \\ &\implies b = ax \quad \text{or} \quad c = ay \quad \text{for some } x, y \in D \\ &\implies a = (ax)c \quad \text{or} \quad a = b(ay) \quad (\text{by the cancellation law and using } a \neq 0) \\ &\implies 1 = xc \quad \text{or} \quad 1 = by \\ &\implies c \in D^\times \quad \text{or} \quad b \in D^\times. \end{aligned}$$

□

We will be using the connections between irreducible and prime elements to show that a PID has the Unique Factorization property.

Definition 19. An integral domain D is called a Unique Factorization Domain (UFD) if every non-zero element a can be written as

$$a = up_1 \dots p_n$$

with $u \in D^\times$ and each p_i irreducible in D , and moreover the ideals $\langle p_i \rangle$ are unique up to reordering.

MATHEMATICS DEPARTMENT, UNIVERSITY OF CALIFORNIA, SAN DIEGO, CA 92093-0112, USA

Email address: golsefidy@ucsd.edu