MATH361 NOTES

JINGWEN FENG

Contents

Date: May 15, 2022.

1. **Week1**

Normality, Quotient Groups and Canonical Projection

Normality, Quotient Groups and Canonical Projection

1.1. **Definitions.** :

▶ $\mathbf{H \leq G}$: H is a subgroup of G.

▶ $\mathbf{H \trianglelefteq G}$: H is a normal subgroup of G. (When $\sim_{l,H}$ and $\sim_{r,H}$ are the same relation: if $\forall g \in G, \forall h \in H, ghg^{-1} \in H$

▶ **Coset multiplication (when $\mathbf{H \trianglelefteq G}$)**:$(g_1H)(g_2H) = (g_1g_2)H$.

▶ **Canonical projection (from G onto G/H)**: Suppose $H \trianglelefteq G$. Define $\pi : G \to G/H$ as follows: $\pi(a) = aH$. Then π is an epimorphism.

1.2. **Theorems.** :

★ **Theorem characterizing when coset multiplication is well-defined**: If H is a normal subgroup of G, Then coset multiplication is well-defined.

★ **Theorem concerning the properties of coset multiplication ("When $\mathbf{H \trianglelefteq G}$, coset multiplication turns G/H into a...")**: If $H \trianglelefteq G$, then G/H is a group under coset multiplication.

★ **Theorem describing the kernel of the canonical projection**: Let $\pi : G \to G/H$ be the canonical projection. Then $ker(\pi) = H$.

★ **Fundamental Theorem of Homomorphisms**: Suppose $\phi : G \to H$ is a homomorphism. Let $\phi : G \to G/Ker(\phi)$ be the canonical projection. Then there exists a unique monomorphism $\widehat{\phi} : G/Ker(\phi) \to H$ such that $\widehat{\phi} \circ \pi = \phi$

1.3. **Notes from last semester (Cosets).** G: a group, $a, b \in G, H \leq G$.

$$a \sim_{l,H} b \iff b^{-1}a \in H$$
$$a \sim_{r,H} b \iff ba^{-1} \in H$$
$$aH = [a]_{\sim_{r,H}} = \{ah \in H, h \in H\} \text{ (left coset)}$$
$$Ha = [a]_{\sim_{r,H}} = \{ha \in H, h \in H\} \text{ (right coset)}$$

(equivalence relations)

1.4. **Equality Test.**

$$aH = bH \iff b^{-1}a \in H$$

1.5. **Subgroup and Normal Subgroup.**

1.5.1. ***Subgroup***.

Definition 1. ***Subgroup***
Suppose $(G, \triangle)$ is a group, $H \leq G$. H is a subgroup of G if

(1) $e \in H$
(2) *if* $h_1, h_2 \in H$, *then* $h_1 \triangle h_2 \in H$
(3) *if* $h \in H$, *then* $h' \in H$

1.5.2. ***Normal Subgroup***.

Definition 2. ***Normal Subgroup***
If $\forall g \in G, \forall h \in H, ghg^{-1} \in H$, then $\sim_{l,H}$ are the same relation. If this happens, H is a normal subgroup of G, $H \trianglelefteq G$.

Normality is rare. But if G is abelian, then normality is automatic.

1.5.3. ***Normality***. **Normality** If $\sim_{l,H}$ and $\sim_{r,H}$ are the same relation.

$$[g]_{\sim_{l,H}} = [g]_{\sim r,H}$$
$$gH = Hg$$
$$ghh'g, (h, h' \in H)$$
$$ghg^{-1} = h$$
$$ghg^{-1} \in H$$
$$gh = h'g(normality)$$

1.6. **Kernels are always normal.**

$$\begin{aligned} G \xrightarrow{\phi} H & \\ \phi(g_1 g_2) &= \phi(g_1)\phi(g_2) \text{ (Homomorphism)} \\ \phi[G] &= im\phi \\ \phi^{-1}[\{e_H\}] &= ker\phi \\ k &\in ker\phi \\ \phi(gkg^{-1}) &= \phi(g)\phi(k)\phi(g^{-1}) \\ \phi(k) &= e_H \\ \phi(gkg^{-1}) &= e_H \in ker\phi \end{aligned}$$

1.7. **Quotient Groups.**

Definition 3. ***Quotient Groups***
Suppose $H \leq G$. Recall that G/H is the collection of left cosets (all aH).

$$G/H = \{gH | g \in G\}$$
$$G\backslash H = \{Hg | g \in G\}$$

These are well-defined sets of G.

If G is abelian. then normality is automatic. ($aH = Ha$).
A set id a well-defined collection objects called elements or members of the set. Well-defined means that any given object must either be an element of the set, or not be an element of the set.

1.8. **Coset Multiplication.**

Definition 4. ***Coset Multiplication***

$$(g_1 H)(g_2 H) = (g_1 g_2)H$$

Theorem 1. ***Charaterizing when coset multiplication is well-defined***
If H is a normal subgroup of G, then coset multiplication is well-defined.

Proof. Suppose $a_1 H = b_1 H$ and $a_2 H = b_2 H$. Prove that $(a_1 a_2)H = (b_1 b_2)H$.

Since $a_1H = b_1H$, $b_1^{-1}a_1 \in H$ say $b_1^{-1}a_1 = h_1$. Similarly, put $b_2^{-1}a_2 = h_2 \in H$.

$$\begin{aligned} a_1 &= b_1h_1 \\ a_2 &= b_2h_2 \\ a_1a_2 &= b_1h_1b_2h_2 \\ &= b_1b_2h_1'h_2 \text{ (normal)} \\ (b_1b_2)^{-1}a_1a_2 &= h_1'h_2 \in H \\ (a_1a_2)H &= (b_1b_2)H \end{aligned}$$

□

Theorem 2. ***Concerning property of coset multiplication*** *if $H \trianglelefteq G$, then G/H is a group under coset multiplication.*

Proof. Associative:

$$\begin{aligned} ((aH)(bH))(cH) &= ((ab)H)(cH) \\ &= ((ab)c)H \\ &= (a(bc))H \\ &= (aH)((bc)H) \\ &= (aH)((bH)(cH)) \end{aligned}$$

Identity:
eH should be an identity, e is the identity of G.

$$\begin{aligned} (aH)(eH) &= (ae)H \\ &= aH \\ (eH)(aH) &= (ea)H = aH \end{aligned}$$

Inversion:
The inverse of aH is $a^{--1}H$

$$\begin{aligned} (aH)(a^{-1}H) &= (aa^{-1})H \\ &= eH \\ (a^{-1}H)(aH) &= (a^{-1}a)H \\ &= eH \end{aligned}$$

□

1.9. **Canonical Projection.**

Definition 5. ***Canonical Projection*** *Suppose $H \trianglelefteq G$. Define $\pi : G \to G/H$ as follows: $\pi(a) = aH$. Then π is an epimorphism.*

Note: epimorphism: homomorphism ($\phi(g_1g_2) = \phi(g_1)\phi(g_2)$) and ϕ is surjective.

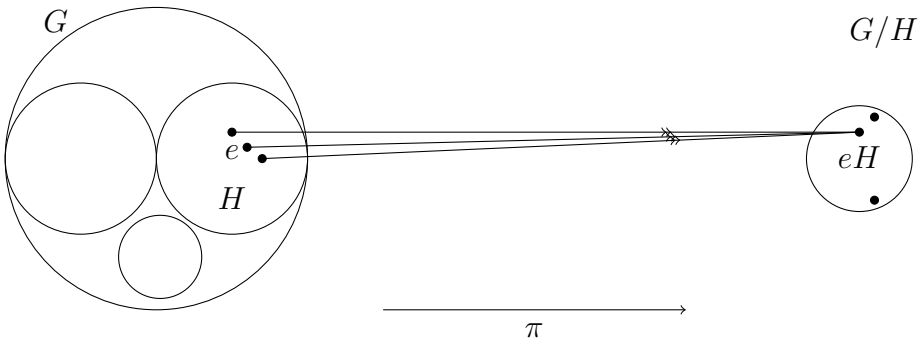
$$\pi(ab) = (ab)H$$
$$\pi(a)\pi(b) = (aH)(bH)$$

These are equal by definition.
Surjective: any element of G/Hhas the form aH. Then $\pi(a) = aH$

Theorem 3. ***Describing Kernel of Canonical Projection***
Let $\pi : G \to G/H$ be the canonical projection, then $ker(\pi) = H$.

Proof.

$$\begin{aligned} ker(\pi) &= \{a \in G | \pi(a) = eH\} \\ &= \{a \in G | aH = eH\} \\ &= \{a \in G | e^{-1}a \in H\} \\ &= \{a \in G | a \in H\} \\ &= H \end{aligned}$$



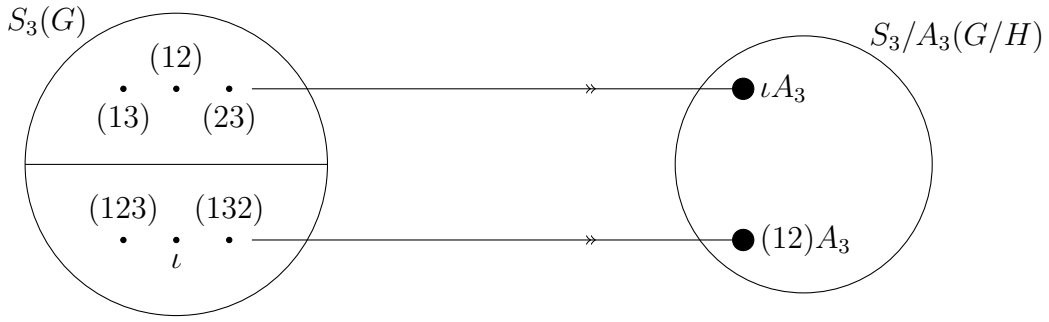
□

Kernels are normal, this shows that coset multiplication cannot be well-defined if H is not normal.

Example 1. *Quotient Groups*

(1) *Quotient Groups*

$$G = S_3, H = A_3$$
$$H = \{\iota, (123), (132)\}$$
$$\iota H = \{\iota, (123), (132)\}$$
$$(12)H = \{(12), (23), (13)\}$$



	ιA_3	$(12)A_3$
ιA_3	ιA_3	$(12)A_3$
$(12)A_3$	$(12)A_3$	ιA_3

(2) ***Bad Example of Quotient Group***

$$G = S_3, H = \langle (12) \rangle$$

$$\begin{aligned} \iota H &= \{\iota, (12)\} \\ (13)H &= \{(13), (123)\} \\ (132)H &= \{(132), (23)\} \\ ((13)H) &= ((123)H) \\ ((13)H)((132)H) &= (132)H \\ ((123)H)((132)H) &= \iota H \\ ((13)H)((132)H) &\neq ((123)H)((132)H) \end{aligned}$$

	ιH	$(13)H$	$(132)H$
ιH	ιH	$(13)H$	$(132)H$
$(13)H$	$(13)H$	ιH	$(132)H$
$(132)H$			

(3) *Order of Quotient Group*

$$\begin{aligned} &\textit{order of } 5 + \langle 4 \rangle \textit{ in } \mathbb{Z}/\langle 4 \rangle \\ &0 + \langle 4 \rangle = \{0, 4, 8\} \\ &1 + \langle 4 \rangle = \{1, 5, 9\} \\ &2 + \langle 4 \rangle = \{2, 6, 10\} \\ &3 + \langle 4 \rangle = \{3, 7, 11\} \end{aligned}$$

	$0+\langle 4\rangle$	$1+\langle 4\rangle$	$2+\langle 4\rangle$	$3+\langle 4\rangle$
$0+\langle 4\rangle$	0	1	2	3
$1+\langle 4\rangle$	1	2	3	0
$2+\langle 4\rangle$	2	3	0	1
$3+\langle 4\rangle$	3	0	1	2

$$5+\langle 4\rangle = 1+\langle 4\rangle$$
$$(5+\langle 4\rangle)^4 = 0+\langle 4\rangle$$

Order is 4.

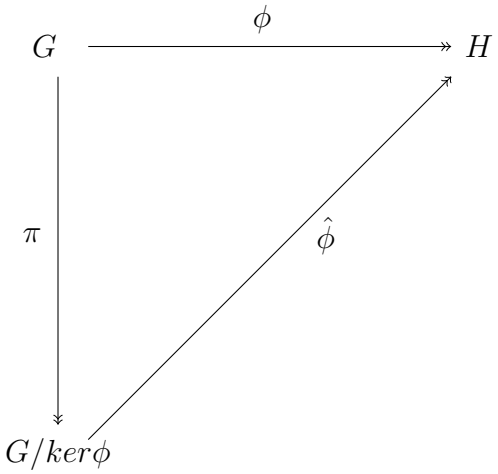
1.10. **How to test for normality.**

(1) Definition: $H \trianglelefteq G$ iff $\forall g \in G, \forall h \in H, ghg^{-1} \in H$.
If G is finite, this is computable using a nested loop:
$for(g : g \in G)\{$
$for(h : h \in H)\{$

(2) Abelian G $\rightarrow$ always normal.
(3) H is a kernel of some homomorphisms.
(4) $[G : H] = 2$.

1.11. **Fundamental Theorem of Homomorphisms.**

Theorem 4. ***Fundamental Theorem of Homomorphisms***
Suppose $\phi : G \rightarrow H$ is a homomorphism.
Let $\pi : G \rightarrow G/Ker\phi$ be the canonical projection. Then there exists a unique monomorphism $\hat{\phi} : G/Ker\phi \rightarrow H$, such that $\hat{\phi} \circ \pi = \phi$.



Proof. (1) (Uniqueness) Suppose that a $\hat{\phi}$ exists.

$$\begin{aligned}\hat{\phi_2}(cker\phi) &= \hat{\phi_2}(\pi(c)) \\ &= (\hat{\phi} \circ \pi)(c) \\ &= \phi(c)\end{aligned}$$

(2) (Existence) "Define" $\hat{\phi}(cker\phi) = \phi(c)$.
But the user get to choose c, so we need to be sure that the RHS is independent of this choice.
Suppose $c_1 ker\phi = c_2 ker\phi$,
Then $c_2^{-1}c_1 \in ker\phi$, say $c_2^{-1}c_1 = k$.

$$\begin{aligned}c_1 &= c_2 k \\ \phi(c_1) &= \phi(c_2 k) \\ &= \phi(c_2)\phi(k) \\ &= \phi(c_2)e_H \\ &= \phi(c_2)\end{aligned}$$

so: $\hat{\phi} = \phi(c)$ is a well-defined formula.
$\hat{\phi}$ preserves operations:

$$\begin{aligned}\hat{\phi}(cker\phi)(dker\phi) &= \phi((cd)ker\phi) \\ &= \phi(cd)\end{aligned}$$

OTOH

$$\phi(cker\phi)\phi(dker\phi) = \phi(c)\phi(d) \text{ homomorphism}$$

Suppose

$$\begin{aligned}\hat{\phi}(cker\phi) &= \hat{\phi}(dker\phi) \\ \phi(c) &= \phi(d) \\ e_H &= (\phi(c))^{-1}\phi(d)\end{aligned}$$

so

$$\begin{aligned}\phi(c^{-1}d) &= e_H \\ c^{-1}d &\in ker\phi \\ dker\phi &= cker\phi\end{aligned}$$

□

2. Week2

2.1. **Definitions.** ▶ **Ring**:A ring is a triple $(R, +, \cdot)$ where R is a set, $+$ and $\cdot$ are binary operations on R.
(1) $(R, +)$ is an abelian group.
(2) $(R, \cdot)$ is a semigroup ($\cdot$ is associative).
(3) We have the left and right distributive laws:
(a) $a \cdot (b + c) = (a \cdot b) + (a \cdot c) \leftarrow$ left distributive law.
(b) $(a + b) \cdot c = (a \cdot c) + (b \cdot c) \leftarrow$ right distributive law.

▶**Identity**(of additive and multiplicative operations): (1)The identity element of $(R, +)$ is called the **zero element** of R, denote $\mathbf{0_R}$.
(2)$(R, \cdot)$ may or may not have an identity element.

▶ **Unital (ring)**: $(R, \cdot)$ may or may not have an identity element. If $(R, \cdot)$ does have an identity, we say that R is a **unital ring** and we refer to the multiplicative identity as the **unity element** of R, denoted $\mathbf{1_R}$.

▶**Inverse**(of additive and multiplicative operations): (1) If $a \in R$, the additive inverse is called the **opposite of** a, denoted $-\mathbf{a}$.
(2) If R is unital, then a may or may not have a multiplicative inverse. If it does, then a is a **unit** and its multiplicative inverse is denoted $\mathbf{a^{-1}}$.

▶**Commutative (ring)**: $(R, \cdot)$ may or may not be commutative. If it is, we say that R is a **commutative ring**.
◦ **Example**: $(M_n(\mathbb{R}), +_n, \cdot_n)$ is a ring;
$0_{M_n(\mathbb{R})}$ = zero matrix ;
$1_{M_n(\mathbb{R})}$ = identity matrix;
not commutative;
Units of $M_n(\mathbb{R})$: invertible matrices.

2.2. **Theorems.** ★ **Rules of sign for rings** (this appears in the text as Theorem 18.8): Let R be any ring. Then:(1)$0_R \cdot a = 0_R = a \cdot 0_R$; (2) $(-a)b = a(-b) = -(ab)$; (3)$(-a)(-b) = ab$.

2.3. **Ring.**

Definition 6. *A ring is a triple $(R, +, \cdot)$ where R is a set, $+$ and $\cdot$ are binary operations on R.*

Definition 7 (Rings)**.** *Properties.*

(1) $(R, +)$ *is an abelian group.*
(2) $(R, \cdot)$ *is a semigroup (*$\cdot$ *is associative).*
(3) *We have the left and right distributive laws:*
   (a) $a \cdot (b + c) = (a \cdot b) + (a \cdot c) \leftarrow$ *left distributive law.*
   (b) $(a + b) \cdot c = (a \cdot c) + (b \cdot c) \leftarrow$ *right distributive law.*

Definition 8 (Identity)**.** *Identity of additive and multiplicative operations.*

(1) *The identity element of* $(R, +)$ *is called the* ***zero element*** *of* R*, denote* $\mathbf{0_R}$.
(2) $(R, \cdot)$ *may or may not have an identity element. If* $(R, \cdot)$ *does have an identity, we say that* R *is a* ***unital ring*** *and we refer to the multiplicative identity as the* ***unity element*** *of* R*, denoted* $\mathbf{1_R}$.

Definition 9 (Inverse)**.** *Inverse of additive and multiplicative operations.*

(1) *If* $a \in R$*, the additive inverse is called the* ***opposite of*** a*, denoted* $-\mathbf{a}$.
(2) *If* R *is unital, then* a *may or may not have a multiplicative inverse. If it does, then* a *is a* ***unit*** *and its multiplicative inverse is denoted* $\mathbf{a^{-1}}$.

Definition 10 (commutative)**.** *Finally,* $(R, \cdot)$ *may or may not be commutative. If it is, we say that* R *is a* ***commutative ring****.*

Example 2. $(\mathbb{Z}, +, \cdot)$ *is a ring.*
$0_{\mathbb{Z}} = 0$
$-(5) = (-5)$
Is unital: $1_{\mathbb{Z}} = 1$
Is commutative.
Units: $1, -1$.

Example 3. $(2\mathbb{Z}, +, \cdot)$ *is a non-unital ring.*
$0_{2\mathbb{Z}} = 0$
Is commutative.

Example 4. $(\mathbb{Z}_n, +_n, \cdot_n)$ *is a ring.*
$0_{\mathbb{Z}_n} = [0]_{\equiv_n}$

$1_{\mathbb{Z}_n} = [1]_{\equiv_n}$
Is commutative.
Units of $\mathbb{Z}_n$*:* $[a]$ *is a unit iff* $gcd(a, n) = 1$.

Example 5. $(Fun(\mathbb{R}, \mathbb{R}), +, \cdot)$ *is a ring.*
$(f + g)(x) = f(x) + g(x)$ *("pointwise addition")*
$(fg)(x) = f(x)g(x)$ *("pointwise multipliaction")*
These operations turn $Fun(\mathbb{R}, \mathbb{R})$ *into a ring.*
$0_{Fun(\mathbb{R},\mathbb{R})} =$ *"zero function:* $f(x) = 0$
$1_{Fun(\mathbb{R},\mathbb{R})} =$ *"one function:* $f(x) = 1$
★ *Is commutative?*

Example 6. $(M_n(\mathbb{R}), +_n, \cdot_n)$ *is a ring.*
$0_{M_n(\mathbb{R})} =$ *zero matrix*
$1_{M_n(\mathbb{R})} =$ *identity matrix*
not commutative.
Units of $M_n(\mathbb{R})$*: invertible matrices.*

Theorem 5. *Let* R *be any ring. Then:*

(1) $0_R \cdot a = 0_R = a \cdot 0_R$
(2) $(-a)b = a(-b) = -(ab)$
(3) $(-a)(-b) = ab$

Proof. (1)

$$\begin{aligned} 0_R + 0_R &= 0_R \\ (0_R + 0_R)a &= 0_R a \\ 0_R a + 0_R a &= 0_R a \\ (0_R a + 0_R a) - 0_R a &= 0_R a - 0_R a \\ 0_R a + (0_R a - 0_R a) &= 0_R \\ 0_R a + 0_R &= 0_R \\ 0_R a &= 0_R \end{aligned}$$

Other half is similar.

(2)

$$\begin{aligned}(-a)b + ab &= (-a + a)b \\ &= 0b \\ &= 0 \\ (-a)b &= -ab\end{aligned}$$

(3)

$$\begin{aligned}(-a)(-b) &= -(a(-b)) \\ &= -(-(ab)) \\ &= ab\end{aligned}$$

□

2.4. **Problems.**

Problem 1. *"(Direct products of groups)" Let G and H be groups. Define a binary operation on the Cartesian product set $G \times H$ by the formula $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$. Show that*
(i) this operation is associative;
(ii) the ordered pair (e_G, e_H) is an identity element for this operation; and
(iii) any ordered pair (g, h) has inverse (g^{-1}, h^{-1}). Thus, with this operation, the Cartesian product $G \times H$ becomes a group, which we call the "direct product" of the groups G and H.

Proof. (1) Associative

$$\begin{aligned}[(g_1, h_1)(g_2, h_2)](g_3, h_3) &= (g_1 g_2, h_1 h_2)(g_3, h_3) \\ &= ((g_1 g_2) g_3, (h_1 h_2) h_3) \\ &= (g_1 (g_2 g_3), h_1 (h_2 h_3)) (G, H \text{ are groups}) \\ &= (g_1, h_1)[(g_2, h_2)(g_3, h_3)]\end{aligned}$$

(2) Identity

$$\begin{aligned}(g, h)(e_G, e_H) &= (g e_G, h e_H) \\ &= (g, h) \\ (e_G, e_H)(g, h) &= (e_G g, e_H h) \\ &= (g, h)\end{aligned}$$

(3) Inverse

$$\begin{aligned}(g, h)(g^{-1}, h^{-1}) &= (g g^{-1}, h h^{-1}) \\ &= (e_G, e_H) \\ (g^{-1}, h^{-1})(g, h) &= (g^{-1} g, h^{-1} h) \\ &= (e_G, e_H)\end{aligned}$$

□

Problem 2. *List the elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$, and then make an operation table for the operation defined above. "(Note: with this we have at last proved that the Klein four-group is really a group, in particular that its operation is really associative.)"*
Elements in $\mathbb{Z}_2 \times \mathbb{Z}_2 : (0,0), (0,1), (1,0), (1,1)$
Operation table:

	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(1,0)$

Problem 3. *Is the direct product group $\mathbb{Z}_2 \times \mathbb{Z}_2$ isomorphic to $\mathbb{Z}_4$? Prove your answer.*

Proof. Operation table of $\mathbb{Z}_4$:

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

In direct product group $\mathbb{Z}_2 \times \mathbb{Z}_2$, there are $(0,0)^2 = (0,0), (0,1)^2 = (0,0), (1,0)^2 = (0,0)$, However, in $\mathbb{Z}_4$, there are only $0^2 = 2, 2^2 = 2$. (Operation failed). It is not isomorphic.

□

Problem 4. *"(Direct products of rings)" Now let R and S be rings. Define two binary operations on the Cartesian product set $R \times S$ by the formulas $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ and $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$. Show that with these operations, $R \times S$ also becomes a ring, also called the "direct product" of R and S.*

Proof. .

(1) Additive Associativity:

$$\begin{aligned}[(r_1, s_1) + (r_2, s_2)] + (r_3, s_3) &= (r_1 + r_2, s_1 + s_2) + (r_3, s_3) \\ &= ((r_1 + r_2) + r_3, (s_1 + s_2) + s_3) \\ &= (r_1 + (r_2 + r_3), s_1 + (s_2 + s_3)) \\ &= (r_1, s_1) + [(r_2, s_2) + (r_3, s_3)]\end{aligned}$$

(2) Additive Identity:

$$(e_R, e_S)$$

(3) Additive Inversion:

$$(r^{-1}, s^{-1})$$

(4) Additive Commutativity:

$$\begin{aligned}(r_1, s_1) + (r_2, s_2) &= (r_1 + r_2, s_1 + s_2) \\ &= (r_2 + r_1, s_2 + s_1) \\ &= (r_2, s_2) + (r_1, s_1)\end{aligned}$$

$(R \times S, +)$ is an abelian group.

(5) Multiplicative Associativity

$$\begin{aligned}[(r_1, s_1)(r_2, s_2)](r_3, s_3) &= (r_1 r_2, s_1 s_2)(r_3, s_3) \\ &= ((r_1 r_2)r_3, (s_1 s_2)s_3) \\ &= (r_1(r_2 r_3), s_1(s_2 s_3)) \\ &= (r_1, s_1)[(r_2, s_2)(r_3, s_3)]\end{aligned}$$

$(R \times S, +)$ is a semigroup.

(6) Distributive Law

$$\begin{aligned}[(r_1, s_1) + (r_2, s_2)](r_3, s_3) &= (r_1 + r_2, s_1 + s_2)(r_3, s_3) \\ &= ((r_1 + r_2)r_3, (s_1 + s_2)s_3) \\ &= (r_1 r_3 + r_2 r_3), (s_1 s_3 + s_2 s_3) \\ &= (r_1 r_3, s_1 s_3) + (r_2 r_3, s_2 s_3) \\ &= (r_1, s_1)(r_3, s_3) + (r_2, s_2)(r_3, s_3)\end{aligned}$$

$$\begin{aligned}(r_1, s_1)[(r_2, s_2) + (r_3, s_3)] &= (r_1, s_1)(r_2 + r_3, s_3 + s_3) \\ &= (r_1(r_2 + r_3), s_1(s_2 + s_3)) \\ &= ((r_1 r_2 + r_1 r_3), (s_1 s_2 + s_1 s_3)) \\ &= (r_1 r_2, s_1 s_2) + (r_1 r_3, s_1 s_3) \\ &= (r_1, s_1)(r_2, s_2) + (r_1, s_1)(r_3, s_3)\end{aligned}$$

$(R, +, \cdot)$ is a ring.

□

Problem 5. *Show that if R and S are both commutative, then so is $R \times S$.*

$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$$

if R and S are both commutative, then

$$\begin{aligned} r_1 r_2 = r_2 r_1, s_1 s_2 = s_2 s_1 \\ (r_1 r_2, s_1 s_2) &= (r_2 r_1, s_2 s_1) \\ &= (r_2, s_2)(r_1, s_1) \end{aligned}$$

Problem 6. *Show that if R and S are both unital, then so is $R \times S$.*

Proof. If R is unital, then $(R, \cdot)$ has an identity 1_R; If S is unital, then $(S, \cdot)$ has an identity 1_S.
Then $(R \times S, \cdot)$ has an identity $1_{R\times S} = (1_R, 1_S)$

$$\begin{aligned} (r_1, s_1)(1_R, 1_S) &= (r_1 1_R, s_1 1_S) \\ &= (r_1, s_1) \\ (1_R, 1_S)(r_1, s_1) &= (1_R r_1, 1_S s_1) \\ &= (r_1, s_1) \end{aligned}$$

□

Problem 7. *Make a multiplication table for the ring $\mathbb{Z}_2 \times \mathbb{Z}_2$, and explicitly identify the unity element of this ring.*

	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,1)$
$(1,0)$	$(0,0)$	$(0,0)$	$(1,0)$	$(1,0)$
$(1,1)$	$(0,0)$	$(0,0)$	$(0,1)$	$(1,1)$

There is no unity element.

Problem 8. *"(Zero-product property fails in direct products)" The real number system has the well-known "zero-product property:" if $xy = 0$ then either $x = 0$ or $y = 0$. Prove that this is "not" true in arbitrary rings, by giving an explicit counterexample in the ring $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Example: $(1, 0)(0, 1) = (0, 0)$

Problem 9. *"(Zero-product property also fails for functions)" Now consider the ring* $\mathrm{Fun}(\mathbb{R},\mathbb{R})$ *with the usual "pointwise" operations that we discussed in class. Show that the zero-product property also fails in this ring, by giving two specific non-zero functions* f *and* g *with* $fg = 0$*. "(Hint: you will almost certainly want* f *and* g *to be "piecewise-defined" functions.)"*

$$\begin{aligned} f(x) &= x, (x \geq 0) \\ f(x) &= 0, (x < 0) \\ g(x) &= -x, (x \leq 0) \\ g(x) &= 0, (x > 0) \\ f(x)g(x) &= 0 \end{aligned}$$

Problem 10. *"(The zero ring)" Suppose* R *is any set with a single element. Show that there is one and only one way of defining binary operations* $+$ *and* $\cdot$ *on* R *which turn* R *into a ring. Make operation tables for* $+$ *and* $\cdot$*. (Any ring with only a single element is called a "zero ring." Once we have defined what we mean by an "isomorphism" of rings, we will prove that all zero rings are isomorphic with one another, and because of this we will sometimes speak of "the" zero ring rather than "a" zero ring.)*

Assume $R = \{k\}$*, then:*

$+$	k
k	$2k$

$\cdot$	k
k	k^2

$2k \in R, k^2 \in R$*, there is only one element* $k \in R$*, therefore,* $2k = k, k = 0; k^2 = k, 0^2 = 0$
$k = 0$ *(or an element which means the same thing as* 0 *)*
$(R,+)$ *is an abelian group, it is a trivial group.*
$(R,\cdot)$ *is associative:* $r \cdot (r \cdot r) = r = (r \cdot r) \cdot r$*.*
Also obeys distribution law.
It is a rin.

Problem 11. *"(The zero ring is unital)" Show that every zero ring is in fact unital. Prove that in any zero ring, one has the surprising equality* $0_R = 1_R$*.*

Proof.

$\cdot$	k_0
k_0	k_0

$\forall a \in R, a \cdot k_0 = a, k_0 \cdot a = a$. k_0 is the zero element 0_R. $0_R = k_0$.
$\forall a \in R, a \cdot k_0 = k_0, k_0 \cdot a = k_0, a^{-1} = k_0$. a is the unity element 1_R, and $a = k_0$. $1_R = k_0$.
$0_R = 1_R$.

□

Problem 12. *"(The zero ring is the only ring in which $0_R = 1_R$)"' Suppose now that R is "any" unital ring in which $0_R = 1_R$. Prove that R has only one element, and is thus a zero ring. "(Hint: you will need to use at least one of the three assertions in the Rules of Sign theorem referenced above.)"*

Proof. Let R be any ring, then $0_R \cdot a = 0_R = a \cdot 0_R, \forall a \in R$.
if $0_R = 1_R$, then
$1_R \cdot a = 0_R = a \cdot 1_R$.
There is only one zero element, therefore, there is only one unity element here. If 1_R is not the inverse of a, $1_R \cdot a \neq 0_R$. If 1_R is the inverse of a, $1_R \cdot a = 0_R$, and $0_R \cdot a = 1_R \cdot a = a = 0_R$. In this case, $a = 0_R$. The ring has to be a zero ring.

□

3. **Week3**

Rings and Fields

3.1. **Definitions.** ▶ **Zero-divisor**: Let R be a ring, and $a \in R$. We say that a is a left zero-divisor (may not be commutative) if 1. $a \neq 0$, and 2. $\exists b \in R$, with $b \neq 0$ but $ab = 0$.
▶ **Integral domain**: An integral domain is a commutative, unital ring, not the zero ring, which has no zero-divisor.
▶ **Field**:A field is a commutative, unital ring, not the zero ring, in which every non-zero element is a unit.
▶ **Subring**: Suppose R is a ring, and $S \subseteq R$. We say that S is a subring of R if: 1. $0_R \in S$ 2. $a, b \in S \Rightarrow a + b \in S$ 3. $a \in S \Rightarrow -a \in S$ 4. $a.b \in S \Rightarrow ab \in S$
▶ **Unital Subring**: A unital subring of a unital ring R is a subring which contains 1_R. This is not the same as a subring which happens to be unital (1_S might be different.
▶ **Zero (a.k.a. "trivial") subring**: Let R be any ring, $S = \{0_R\}$ is a subring. The zero subring or the trivial subring. This is the smallest subring.
▶ **Improper subring**: et R be any ring, $S = R$ is a subring. The improper subring. This is the largest subring.
▶ **Subring generated by a subset**: Let R be a ring, $A \subseteq R$ be any subset. The subring generated by A is the intersection of all substring containing A.
▶ **Prime subring (of a unital ring)**: Suppose R is any unital ring. The prime subring of R is the subring generated by 1_R. This is the smallest unital subring.

3.2. **Theorems.** ★ Zero-product property (of integral domains): if D is an **integral domain**, and $a, b \in D$ with $ab = 0$, then either $a = 0$ or $b = 0$.
★ Cancellation law (in integral domains): Suppose D is a domain, $a \neq 0$, and $ab = ac$. Then $b = c$.
★ Theorem relating fields to integral domains: Every field is an integral domain.
★ Theorem characterizing the units and zero-divisors of $\mathbb{Z}_n$: Suppose $[a] \in \mathbb{Z}$ and $[a] \neq 0$. Then, 1. If $gcd(a, n) = 1$, then $[a]$ is a unit of $\mathbb{Z}_n$. 2. If $gcd(a, n) \neq 1$, then $[a]$ is a zero-divisor of $\mathbb{Z}_n$.
★ Theorem characterizing when $\mathbb{Z}_n$ is a field, and when it is an integral domain: If n is prime, then $\mathbb{Z}_n$ is a field. If n is composite, then $\mathbb{Z}_n$ is

not even an integral domain.

3.3. **Notes.**

3.3.1. ***Zero divisor***.

Definition 11. *Let R be a ring, and $a \in R$. We say that a is a* ***left zero-divisor*** *(may not be commutative) if*

(1) $a \neq 0$, *and*
(2) $\exists b \in R$, *with* $b \neq 0$ *but* $ab = 0$.

Explanation
Problem: In a general unital ring, solve the equation $x^2 = x$.
Solve using zero-product property in high school:

$$\begin{aligned} x^2 &= x \\ x^2 - x &= 0 \\ x(x - 1_R) &= 0_R \\ x = 0 \text{ or } x - 1 &= 0 \end{aligned}$$

Potential solutions: $x = 0$ or $x = 1$
check: $0^2 = 0 \cdot 0 = 0$
$1^2 = 1 \cdot 1 = 1$

However, now we solve the problem in $\mathbb{Z}_6$:

x	x^2
0	0
1	1
2	4
3	3
4	4
5	1

In $\mathbb{Z}_6$, $0, 1, 3, 4$ are all solutions. We are missing solutions $3, 4$ by using zero-product property in high school.
WARNING: In some rings, techniques of High School Algebra may miss some solutions.
Reaction: $\mathbb{Z}_6$ is a bad ring, because High School Algebra doesn't really work there.)

Example of left zero-divisors in $\mathbb{Z}_6$:

$$\begin{aligned}
&0 : N \\
&1 : N \\
&2 : Y, 2 \cdot 3 = 0 \\
&3 : Y, 3 \cdot 2 = 0 \\
&4 : Y, 4 \cdot 3 = 0 \\
&5 : N
\end{aligned}$$

We are most concerned with the commutative case, and here there is no distinction between left and right zero-divisors.

3.3.2. *Integral Domain*.

Definition 12. *An **integral domain** is a commutative, unital ring, not the zero ring, which has no zero-divisor.*

Example: $\mathbb{Z}_5$ has no zero-divisor.
Find the zero-divisors in $\mathbb{Z}_5$:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

There is no zero-divisor according to the table.
$\mathbb{Z}_5$ is an integral domain; $\mathbb{Z}_6$ is not an integral domain.

3.3.3. *Zero-Product Property*.

Theorem 6. ***Zero-Product Property***
*If D is an **integral domain**, and $a, b \in D$ with $ab = 0$, then either $a = 0$ or $b = 0$.*

3.3.4. *Cancellation Law*.

Theorem 7. ***Cancellation Law***
Suppose D is a integral domain, $a \neq 0$, and $ab = ac$. Then $b = c$.

Proof.

$$\begin{aligned} ab &= ac \\ ab - ac &= 0 \\ a(b-c) &= 0 \\ b - c &= 0 \\ b &= c \end{aligned}$$

□

3.3.5. ***Units and "Divition"***.
it is very rare for 0 to have inverse.

3.3.6. ***Zero Ring and Inverse***.

Theorem 8. *If R is any unital ring in which 0 has a multiplication inverse, then $R = \{0\}$.*

Proof. Suppose 0 has an inverse.

$$0 = 0 \cdot 0^{-1} = 1$$

□

3.4. **Fields.**

Definition 13. *A **field** is a commutative, unital ring, not the zero ring, in which every non-zero element is a unit.*

Example 7.

$$\mathbb{Q}$$

$$1_{\mathbb{Q}} = \frac{1}{1}$$

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

$$\mathbb{R}, \mathbb{C}$$

Example 8. *Non-example $\mathbb{Z}$*
only units are 1 and -1
$\mathbb{Z}$ is not a field.

If we are in a field, we may speak of "diviing by a". This means multiplying by a^{-1}.

3.4.1. ***Fields and Integral Domain.***

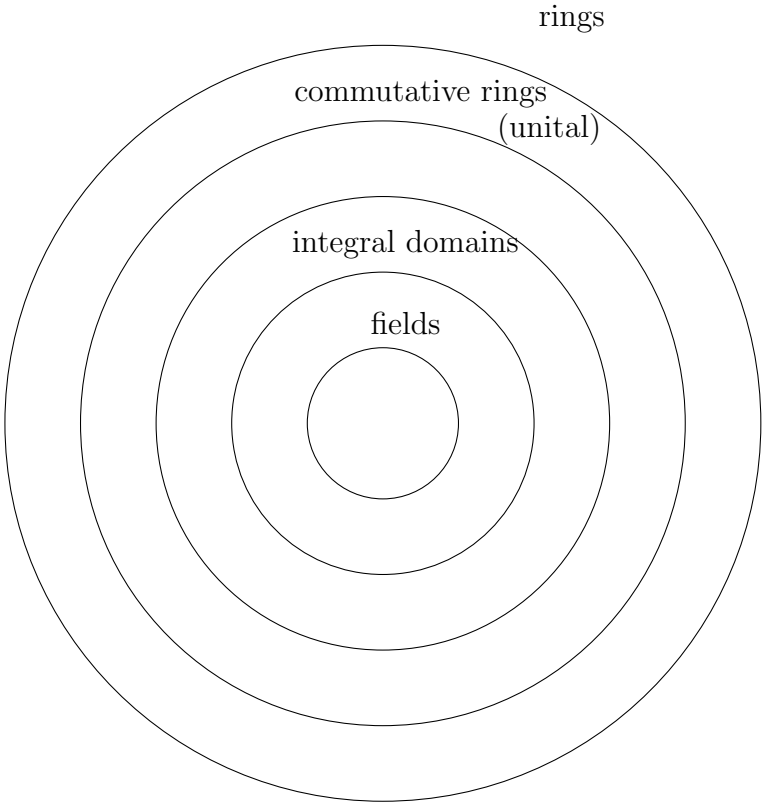
Theorem 9. *Every field is an integral domain.*

Proof. Suppose F is a field.
Need to prove: there are no zero-divisor.
Suppose to the contrary that $a \in F$ is a zero-divisor. Then $a \neq 0$ and $\exists b \neq 0$ with

$$\begin{aligned} ab &= 0 \\ a^{-1}(ab) &= a^{-1}0 \\ b &= 0 \text{ (contradiction) .} \end{aligned}$$

□

3.5. **Universe of Ring Theory.**



Where does $\mathbb{Z}_n$ appear on this map?

3.6. **Unit and Zero-Divisor of $\mathbb{Z}_n$.**

Theorem 10. *Suppose $[a] \in \mathbb{Z}$ and $[a] \neq 0$. Then,*

(1) *If $gcd(a,n) = 1$, then $[a]$ is a unit of $\mathbb{Z}_n$.*
(2) *If $gcd(a,n) \neq 1$, then $[a]$ is a zero-divisor of $\mathbb{Z}_n$.*

Proof.

$$\begin{aligned}[a][\frac{n}{gcd(a,n)}] &= [\frac{an}{gcd(a,n)}] \\ &= [\frac{a}{gcd(a,n)}][n]\end{aligned}$$

when $gcd(a,n) \neq 1, \frac{a}{gcd(a,n)} \in \mathbb{Z}$

$$\begin{aligned}\frac{a}{gcd(a,n)} &= k \\ [k][0] &= [k0] \\ &= [0]\end{aligned}$$

□

Remark: In $\mathbb{Z}_n$, every element is either **zero**, or a **unit**, or a **zero-divisor**.
DON'T BE FOOLED: This is NOT true in general rings. For example: in $\mathbb{Z}$, 2 is not zero, not a unit, and not a zero-divisor.

Example 9. $\mathbb{Z}_{23}$
everything other than 0 will be a unit, because 23 is prime.

Corollary 1. *If n is **prime**, then $\mathbb{Z}_n$ is a field. If n is composite, then $\mathbb{Z}_n$ is **not** even an integral domain.*

Remark: $\mathbb{Z}_p$ is a field. We can do $+, -, \cdot, \div$. There, least familiar aspect is inversion. Done on computers with the **Extended Euclidean Algorithm**.

3.6.1. ***Extended Euclidean Algorithm to find inverse in $\mathbf{Z_n}$.***
In $\mathbb{Z}_n$, compute:

$$\begin{gathered}(a,n) \mapsto (gcd(a,n), x, y) \\ ax + ny = gcd(a,n) \\ [x] = [a]^{-1} \text{ in } \mathbb{Z}_n\end{gathered}$$

Remark: Almost all of Linear Algebra works without modification if scalars and matrix entries come from an arbitrary field. (Concepts and

algorithms involving inner products (dot products) can develop subtle bugs.

3.7. **Substrings.**

Definition 14. ***Subrings***
Suppose R is a ring, and $S \subseteq R$. We say that S is a subring of R if:

(1) $0_R \in S$
(2) $a, b \in S \Rightarrow a + b \in S$
(3) $a \in S \Rightarrow -a \in S$
(4) $a.b \in S \Rightarrow ab \in S$

Example 10. *$2\mathbb{Z}$ is a subring of $\mathbb{Z}$*
Note: a substring of a unital ring might not be unital. $\mathbb{Z}$ is a unital ring with the identity $1_{\mathbb{Z}} = 1$. However, $2\mathbb{Z}$ does not have an identity. $2\mathbb{Z}$ is not a unital ring.

Example 11. $R = \mathbb{Z} \times \mathbb{Z}$, $S = \{(x, 0) | x \in \mathbb{Z}\}$
$S \leq R$
R is unital, $1_R = (1, 1)$
S is unital, $1_S = (1, 0)$
$1_R \neq 1_S$

3.8. **Unital Substrings.**

Definition 15. ***Unital Subring***
A unital subring of a unital ring R is a subring which contains 1_R. This is not the same as a subring which happens to be unital (1_S might be different.

3.9. **Zero/Trivial Substrings.**

Example 12. *Let R be any ring, $S = \{0_R\}$ is a subring. The* ***zero subring*** *or the* ***trivial subring****. This is the smallest subring.*

3.10. **Improper Substrings.**

Example 13. *Let R be any ring, $S = R$ is a subring. The* ***improper subring****. This is the largest subring.*

Definition 16. ***Subring generated by a subset***
Let R be a ring, $A \subseteq R$ be any subset. The subring generated by A is the intersection of all substring containing A.

3.11. **Prime Substrings.**

Definition 17. *Suppose R is any unital ring. The* ***prime subring*** *of R is the subring generated by 1_R. This is the smallest unital subring.*

Example 14. $R = \mathbb{Q}$

$$\left\langle \{\frac{1}{1}\} \right\rangle = \{\cdots, -\frac{1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{2}{1}, \cdots\} = \mathbb{Z}$$

3.12. **Problems.**

Problem 13. *Book Problem 1*
Find all solutions of the equation $x^3 - 2x^2 - 3x = 0$ *in* $\mathbb{Z}_{12}$.
Using Mods.java (function temp1) to calculate:
jingwens-MBP:src jingwenfeng javac Mods.java
jingwens-MBP:src jingwenfeng java Mods 12
0 3 5 8 9 11

Problem 14. *Book Problem 2*
Solve the equation $3x = 2$ *in the field* $\mathbb{Z}_7$*; in the field* $\mathbb{Z}_{23}$.
(function temp2)
jingwens-MBP:src jingwenfeng java Mods 7
3
jingwens-MBP:src jingwenfeng java Mods 23
16

Problem 15. *Book Problem 3*
Find all solutions of the equation $x^2 + 2x + 2 = 0$ *in*$\mathbb{Z}_6$.
(function temp3)
jingwens-MBP:src jingwenfeng java Mods 7
No solution

Problem 16. *Book Problem 4*
Find all solutions of the equation $x^2 + 2x + 4 = 0$ *in*$\mathbb{Z}_6$.
(function temp4)
jingwens-MBP:src jingwenfeng java Mods 6
2

Problem 17. *Book Problem 14*
Show that the matrix $\begin{bmatrix}1 & 2\\ 2 & 4\end{bmatrix}$ *is a divisor of zero in* $M_2(\mathbb{Z})$.

$$\begin{bmatrix}1 & 2\\ 2 & 4\end{bmatrix}\begin{bmatrix}a & b\\ c & d\end{bmatrix} = \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

$$\begin{cases} a + 2c = 0 \\ b + 2d = 0 \end{cases}$$

$$\begin{cases} a = -2c \\ b = -2d \end{cases} \Rightarrow \begin{bmatrix}1 & 2\\ 2 & 4\end{bmatrix} \textit{ is a left zero divisor}$$

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1 & 2\\ 2 & 4\end{bmatrix} = \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

$$\begin{cases} a + 2b = 0 \\ 2c + 4d = 0 \end{cases}$$

$$\begin{cases} a = -2b \\ c = -2d \end{cases} \Rightarrow \begin{bmatrix}1 & 2\\ 2 & 4\end{bmatrix} \textit{ is a right zero divisor}$$

Problem 18. *Describe the prime subrings of* $\mathbb{Q}$*, of* $\mathbb{R}$*, and of* $\mathbb{C}$.
Answer: $\mathbb{Z}$

Problem 19. *Describe the prime subring of* $\mathbb{Z}$.
Answer: $\mathbb{Z}$

Problem 20. *Describe the prime subring of* $\mathbb{Z}_n$.
Answer: Z_n
In $Z_n, \langle 1\rangle = \{0, 1, 2, 3, \cdots n-1\}$

Problem 21. *Working in the field* $\mathbb{Z}_3$*, solve the equation* $x^3 = x$.

$$0 * 0 * 0 = 0$$

$$1 * 1 * 1 = 1$$

$$2 * 2 * 2 = 8 = 2(mod 3)$$

Answer: 0, 1, 2

Problem 22. *Working in the field $\mathbb{Z}_5$, solve the equation $x^5 = x$.*
Answer: $0, 1, 2, 3, 4$

Problem 23. *Working in the field $\mathbb{Z}_7$, solve the equation $x^7 = x$.*
Answer: $0, 1, 2, 3, 4, 5, 6$

Problem 24. *By now you probably have a conjecture about $\mathbb{Z}_{11}$. Do not try to prove this. Instead, prove the conjecture for $\mathbb{Z}_p$ where p is an arbitrary prime. "(Hint: the conjecture is obviously true if $x = 0$. Otherwise x is an element of the group of units of $\mathbb{Z}_p$ (why?). But as we have seen, Lagrange's Theorem implies that in "any" group G we have $g^{|G|} = e$ for every $g \in G$. This gives rise to a certain identity for non-zero elements of $\mathbb{Z}_p$. Multiplying both sides of this identity by x will prove the conjecture.)"*

$$\begin{aligned} R = \mathbb{Z}_p/\{0\} \text{ is a cyclic group} \\ g^{|\mathbb{R}|} = e, g \in \mathbb{R} \\ |\mathbb{R}| = p - 1 \\ g^{p-1} = e \\ gg^{p-1} = ge \\ gg^{-1}g^p = ge \\ g^p = g \end{aligned}$$

Problem 25. *Show by a simple counterexample (e.g. in $\mathbb{Z}_6$) that the result above is "not" generally true in $\mathbb{Z}_n$ when n is composite. Exactly which part of your proof above breaks in the composite case?*

$$gg^{-1}g^p = ge$$

However, g is a zero-divisor when $gcd(g, n) \neq 1$ and g doesn't have an inverse. We are not able to find g^{-1}.

Problem 26. *Try to correctly generalize the conjecture to the composite case (i.e. formulate and prove a statement which encompasses the prime case but is also true in the composite case). In doing this you will be following in the footsteps of Leonhard Euler; this result (like many others) is known as "Euler's Theorem," and it is in fact the mathematical basis of RSA encryption.*

$$g^n = g \text{ when } gcd(g, n) = 1, g \in \mathbb{Z}_n \text{ (or } g = 0)$$

4. Week4

4.1. **Definitions.** ▶ Homomorphism (of rings): Suppose R, S are rings. A function $\phi : R \to S$ is a homomorphism (or morphism) if

(1) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$
(2) $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$

$\forall r_1, r_2 \in R$. A morphism is said to be a monomorphism if it's injective.

A morphism is said to be a epimorphism if it's surjective.

A morphism is said to be an isomorphism if it's bijective.

▶ Unital homomorphism (of unital rings): A morphism ϕ between unital rings is said to be a unital morphism if $\phi(1_R) = 1_S$.

▶ Pushforward (of a subring under a homomorphism; a.k.a. "forward image"):

Suppose $f : A \to B$ is a function, $C \subseteq A$, then $f[c] = \{f(c)|c \in C\}$ (pushforward of C).

▶ Pullback (of a subring under a homomorphism; a.k.k. "preimage"):

Suppose $f : A \to B$ is a function, $D \subseteq B$, then $f^{-1}[D] = \{a \in A|f(a) \in D\}$ (pushforward of C).

▶ Image (of a ring homomorphism): $\phi[R] = im\phi$

▶ Kernel (of a ring homomorphism): $\phi^{-1}[\{0_S\}] = ker\phi$

▶ Ideal: Let R be any ring. A **left ideal** of R is a subring $I \leq R$ which absorbs left products from$R$ (if $i \in I$ and $e \in R$ then also $ri \in I$). If I is simultaneosly a ;eft and a right ideal, then I is an ideal.

▶ R/I (the "quotient" of the ring R by the two-sided ideal I): Suppose R is a ring. and I is an ideal of R. Then $(I, +) \trianglelefteq (R, +)$
$[a] = a + I := \{a + r : r \in I\}$
R/I becomes a quotient ring if:

(1) $(a + I) + (b + I) = (a + b) + I$
(2) $(a + I)(b + I) = (ab) + I$

From group theory: R/I is a group under coset addition.

▶ Addition (in R/I, i.e. coset addition): $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$

▶ Multiplication (in R/I, i.e. coset multiplication): $(r_1+I)(r_2+I) = (r_1 r_2) + I$

▶ **Principal Ideals**: Let R be any unital ring, and let $a \in R$. Define $Ra = \{ra|r \in R\}$. Ra is a left ideal, and is in fact the smallest left ideal that contains a.

4.2. **Theorems.** ★ Theorem concerning $\phi(0_R)$, where $\phi : R \to S$ is a ring homomorphism: f $\phi : R \to S$ is a morphism, then $\phi(0_R) = 0_S$. BUT $\phi(1_R)$ may or may not be 1_R.

★ Examples of ring homomorphisms $\phi : R \to S$ to show that $\phi(1_R)$ "may or may not" equal 1_S, even when R and S are both unital: If $\phi : R \to S$ is a morphism, then $\phi(0_R) = 0_S$. BUT $\phi(1_R)$ may or may not be 1_R.

Proof. Note that $(R, \cdot_R)$ and $(S, \cdot_S)$ are usually semigroups. They are usually not groups.
$\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, \phi(n) = (n, 0); \phi(1) = (1, 0) \neq (1, 1)$. □

★ Theorem characterizing the properties of the pushforward of a subring (i.e. "The pushforward of a subring is a..."): Suppose $\phi : R \to S$ is a morphism.
if $T \leq R$, then $\phi[T] \leq S$ (If we push forward a subring, we get another subring on the other side).
If $U \leq S$ then $\phi^{-1}[U] \leq R$.

★ Theorem characterizing the properties of the pullback of a subring (i.e. "The pullback of a subring is a..."): $\phi[R] = im\phi$
$\phi^{-1}[\{0_S\}] = ker\phi$
Note:
ϕ is epimorphism $iff im\phi = S$
ϕ is monomorphism $iff ker\phi = \{0_R\}$
(Already proved this for groups.)

★ Kernels-Absorb-Products-Theorem: Suppose $\phi : R \to S$ is a morphism. If $k \in ker\phi$ and $r \in R$ then $rk \in ker\phi$ and $kr \in ker\phi$.

★ Theorem characterizing the special properties of kernels (i.e. "Kernels absorb..." or "Kernels are..."): Kernels are ideals.

★ Theorem characterizing ideals which contain units: Suppose I is an ideal of R which contains a unit, then $I = R$.

★ Theorem characterizing the ideals of a field: In any field F, the only ideals are $\{0\}$ and F.

★ Theorem characterizing when coset multiplication is well-defined (i.e. "Multiplication in R/I is well-defined provided that I is an..."): When I is an ideal, multiplication in R/I is well-defined.

★ Equality test for elements of R/I: Choose any two elements $r_1 + I$ and $r_2 + I$. If $r_1 - r_2 \in I$, then $r_1 + R = r_2 + R$.

★ If R is a ring and I is an ideal of R, then R/I is a ring under coset + and coset$\cdot$. If R is commutative, so is R/I. If R is unital, so is R/I.

4.3. **Homomorphisms.**

Definition 18. ***Homomorphism*** *Suppose R, S are rings. A function $\phi : R \to S$ is a homomorphism (or morphism) if*

(1) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$
(2) $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$

$\forall r_1, r_2 \in R$.

A morphism is said to be a monomorphism if it's injective.

A morphism is said to be a epimorphism if it's surjective.

A morphism is said to be an isomorphism if it's bijective.

Example 15. $\pi : \mathbb{Z} \to \mathbb{Z}_n, \pi(j) = [j]_{\equiv_n}$

$$\begin{aligned} \pi(j+k) &= [j+k] \\ &= [j] + [k] \\ &= \pi(j) + \pi(k) \\ \pi(jk) &= [jk] = [j][k] \end{aligned}$$

This is an epimorphism.
Observe: $\pi(0_{\mathbb{Z}}) = 0_{\mathbb{Z}_n}$
$\pi(1_{\mathbb{Z}}) = 1_{\mathbb{Z}_n}$

Example 16. *Let R and S be arbitrary rings. Define*
$\pi_1 : R \times S \to R$
$\pi_1((r, s)) = r$
π_1 is a morphism.

$$\begin{aligned} &\pi_1((r_1, s_1) + (r_2, s_2)) \\ &\qquad = \pi_1((r_1 + r_2, s_1 + s_2)) \\ &\qquad = r_1 + r_2 \\ &\qquad = \pi_1((r_1, s_1)) + \pi_1((r_2, s_2)) \end{aligned}$$

This is an epimorphism. (It is injective only if S is a zero ring.)

Example 17. *Let R and S be arbitrary rings. Define*
$\iota : R \to R \times S$ *by* $\iota(r) = (r, 0_S)$

Check:

$$\begin{aligned}\iota(r_1 + r_2) &= (r_1 + r_2, 0_S)\\ \iota(r_1) + \iota(r_2) &= (r_1, 0_S) + (r_2, 0_S)\\ &= (r_1 + r_2, 0_S)\end{aligned}$$

This is an monomorphism. Epimorphism only when $S = \{0_S\}$

$$\begin{aligned}\iota(0_R) &= (0_R, 0_S) = 0_{R\times S}\\ \iota(1_R) &= (1_R, 0_S) \neq 1_{R\times S}\end{aligned}$$

(unless $S = \{0_S\}$*)*

4.3.1. ***Theorem concerning*** $\phi 0_R$).

Theorem 11. *If* $\phi : R \to S$ *is a morphism, then* $\phi(0_R) = 0_S$*. BUT* $\phi(1_R)$ *may or may not be* 1_R*.*

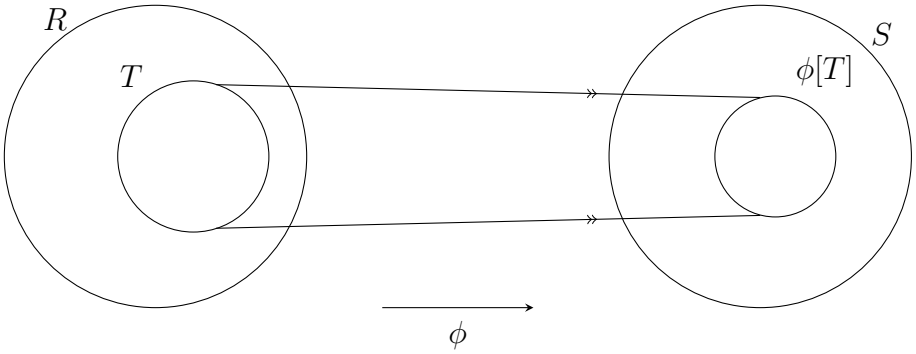
Proof. $(R, +_R)$ and $(S, +_S)$ are groups. Also ϕ is a group morphism. We've already proved that these take e to e.
Note that $(R, \cdot_R)$ and $(S, \cdot_S)$ are usually semigroups. They are usually not groups.

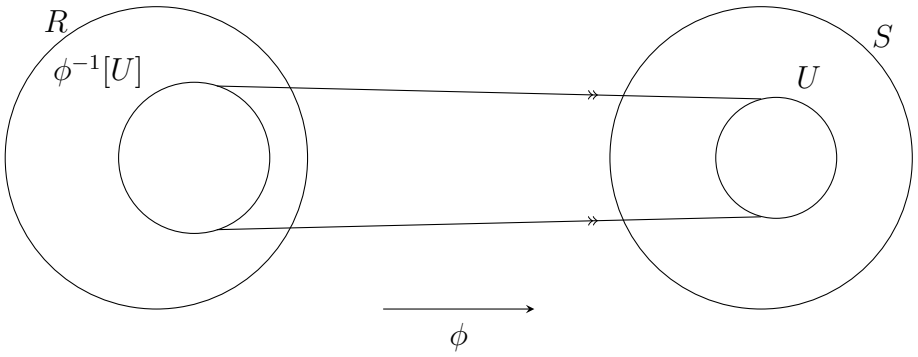
□

4.3.2. ***Unital Morphism***.

Definition 19. ***Unital Morphism***
A morphism ϕ *between unital rings is said to be a unital morphism if* $\phi(1_R) = 1_S$*.*

4.4. **Push forward and Pullback.** .





Definition 20. ***Push forward and Pullback***
Suppose $\phi : R \to S$ is a morphism.
if $T \leq R$, then $\phi[T] \leq S$ (If we push forward a subring, we get another subring on the other side).
If $U \leq S$ then $\phi^{-1}[U] \leq R$.
$\phi[R] = im\phi$
$\phi^{-1}[\{0_S\}] = ker\phi$
Note:
ϕ is epimorphism $iff im(\phi) = S$
ϕ is monomorphism $iff ker(\phi) = \{0_R\}$
(Already proved this for groups).

Theorem 12. ***Kernels-Absorb-Products-Theorem***
Suppose $\phi : R \to S$ is a morphism. If $k \in ker\phi$ and $r \in R$ then $rk \in ker\phi$ and $kr \in ker\phi$.

Proof.

$$\begin{aligned} \phi(k) &= 0_S \\ \phi(rk) &= \phi(r)\phi(k) \\ &= \phi(r)\phi(k) \\ &= \phi(r)0_S \\ &= 0_S \end{aligned}$$

so $rk \in ker(\phi)$ □

Example 18. *$\mathbb{Z}$ is a substring of $\mathbb{R}$, but $\mathbb{Z}$ can NEVER be a kernel of any homomorphism defined on $\mathbb{R}$.*
$\mathbb{Z}$ does not absorb products from$\mathbb{R}$:

$$1 \in \mathbb{Z}$$
$$\frac{1}{2} = \mathbb{R}$$
$$(\frac{1}{2})(1) \notin \mathbb{Z}$$

Definition 21. ***Ideal*** *Let R be any ring. A* ***left ideal*** *of R is a subring $I \leq R$ which absorbs left products fromR (if $i \in I$ and $r \in R$ then also $ri \in I$).*
If I is simultaneosly a ;eft and a right ideal, then I is an ideal.

Theorem 13. *Kernels are ideals.*

A big class of examples - principal ideals.

Definition 22. ***Principal Ideals***
Let R be any unital ring, and let $a \in R$. Define $Ra = \{ra | r \in R\}$

Theorem 14. *Ra is a left ideal, and is in fact the smallest left ideal that contains a.*

Proof. $0 \in Ra$ because $0 = 0a$.
Suppose $x_1, x_2 \in Ra$. Write

$$x_1 = r_1 a, x_2 = r_2 a$$

$$\begin{aligned} x_1 + x_2 &= r_1 a + r_2 a \\ &= (r_1 + r_2)a \\ &\in Ra \end{aligned}$$

Ra absorbs left products:
$x \in Ra$ and $r \in R$
$x = r'a, r \in R$ (some $s \in R$)
$rx = r(r'a) = (rr')a \in Ra$.
Ra is the principle left ideal generated by a. Ra contains a: $a = 1_R \cdot a$.
□

Example 19. *(in $\mathbb{Z}$)*

$$\begin{aligned} \mathbb{Z}0 &= \{0\} = 0\mathbb{Z} \\ 1\mathbb{Z} &= \{\cdots, -1, 0, 1, 2, 3, \cdots\} = \mathbb{Z} \\ (-1)\mathbb{Z} &= \mathbb{Z} \\ 2\mathbb{Z} &= \{\cdots, -2, 0, 2, 4, 6, \cdots\} \end{aligned}$$

Example 20. *(in $\mathbb{R}$)*

$$0\mathbb{R} = \{0\}$$
$$1\mathbb{R} = \mathbb{R}$$
$$(-1)\mathbb{R} = \mathbb{R}$$
$$\frac{1}{2}\mathbb{R} = \mathbb{R}$$
$$2\mathbb{R} = \mathbb{R}$$

In general, $\mathbb{R}u = \mathbb{R}$ for any unit u.

Proof. $Ru \subseteq R$ by definition (R is closed under its own $\cdot$). Other direction: choose any $r \in R$. Then $r = (ru^{-1})u \in Ru$. □

Theorem 15. *Suppose I is an ideal of R which contains a unit, then $I = R$.*

Proof. Suppose $u \in I$ is a unit. Choose any $r \in R$. Then $r = (ru^{-}1)u \in I$. $(ru^{-1} \in R, u \in I)$.

□

Corollary 2. *In any field F, the only ideals are $\{0\}$ and F.*
ideals of $\mathbb{Z} : n\mathbb{Z}(n \geq 0)$

4.5. **Quotient Rings.**

Definition 23. ***Quotient Rings***
Suppose R is a ring. and I is an ideal of R. Then $(I, +) \trianglelefteq (R, +)$
From group theory: R/I is a group under coset addition.

Definition 24. $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$ *(from group theory: R/I is a group under coset addition)*

$$(r_1 + I)(r_2 + I) = (r_1 r_2) + I$$

Might not be well-defined: $(R, \cdot)$ is not a group.

Theorem 16. *When I is an ideal, this operation is well-defined.*

Proof. Soppose

$$r_1 + I = s_1 + I$$

and

$$r_2 + I = s_2 + I$$

Then

$$r_1 - s_1 \in I$$

say $r_1 - s_1 = i_1$

$$r_2 - s_2 \in I$$

say $r_2 - s_2 = i_2$

$$\begin{aligned} r_1 &= i_1 + s_1 \\ r_2 &= i_2 + s_2 \\ r_1 r_2 &= (i_1 + s_1)(i_2 + s_2) \\ &= (i_1 + s_1)i_2 + (i_1 + s_1)s_2 \\ &= i_1 i_2 + s_1 i_2 + i_1 s_2 + s_1 s_2 \\ r_1 r_2 &= s_1 s_2 \end{aligned}$$

anything with i are in I.
Therefore, $r_1 r_2 - s_1 s_2 \in I$
$(r_1 r_2) + I = (s_1 s_2) + I$ □

Theorem 17. *If R is a ring and I is an ideal of R, then R/I is a ring under coset $+$ and coset$\cdot$. If R is commutative, so is R/I. If R is unital, so is R/I.*

Proof. The unity of R/I is $1_R + I$:

$$\begin{aligned} (1_R + I)(a + I) &= (1_R a) + I = a + I \\ (a + I)(1_R + I) &= (a 1_R) + I = a + I \end{aligned}$$

□

Example 21. $R = \mathbb{Z}, I = 3\mathbb{Z}$.

$+$	$0+I$	$1+I$	$2+I$
$0+I$	$0+I$	$1+I$	$2+I$
$1+I$	$1+I$	$2+I$	$0+I$
$2+I$	$2+I$	$0+I$	$1+I$

$\cdot$	$0+I$	$1+I$	$2+I$
$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$2+I$
$2+I$	$0+I$	$1+I$	$1+I$

Remark 1: $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Remark 2: $\mathbb{Z}$ was an integral domain. $\mathbb{Z}/p\mathbb{Z}$ is a field. But if n is composite, then $\mathbb{Z}/n\mathbb{Z}$ is not even an integral domain.

Example 22. *Take $R = \mathbb{R}[x]$. This means the ring of* ***polynumial functions*** *from $\mathbb{R}$ to $\mathbb{R}$.*

e.g.

$$\frac{3}{2}x^5 + 2x - 5 \in \mathbb{R}[x]$$
$$3x + 4x^{-1} \notin \mathbb{R}[x]$$
$$sin(x^2 + 1) \notin \mathbb{R}[x]$$

Also take $I = (\mathbb{R}[x])(x^2 + 1)$

$$1_{R/I} = 1 + I$$
$$-1_{R/I} = -1 + I$$
$$\alpha = x + I$$
$$\alpha^2 = (x = I)(x + I)$$
$$= x^2 + I$$

Equality test for cosets ($b^{-1}a \in I$)*:*

$$x^2 - (-1) = x^2 + 1$$
$$= 1(x^2 + 1) \in I$$
$$\text{so: } \alpha^2 = -1 \text{ (in } R[x]/\left\langle x^2 + 1 \right\rangle)$$

This α *is usually denoted* i*. And* $R/I = \mathbb{C}$*.*

Example 23. *Take* $R = \mathbb{R}[x]$*; take* $I = ([x])(x^2 - 1)$
In R/I*, take* $\alpha = (x + 1) + I, \beta = (x - 1) + I$*.*
$\alpha\beta = ((x + 1) + I)((x - 1) + I) = (x^2 - 1) + I = 0 + I$*.*
(Take the difference of (x^2-1) *and* 0 *to see if it is in* $I = (\mathbb{R}[x])(x^2-1)$*).*
Is $\alpha = 0$*?*
$x + 1 - 0 = x + 1$*. Is this a multiple of* $x^2 - 1$*? No. So* $a \neq 0$*. Also* $\beta \neq 0$*.*
This R/I *is not an integral domain.*

(1) $\mathbb{Z}/n\mathbb{Z}$: field if n is prime, not integral domain if n is composite.
(2) $\mathbb{R}[x]/(x^2 + 1)$ is a field.
(3) $\mathbb{R}[x]/(x^2 - 1)$ is not an integral domain.

4.6. **Problems.**

Problem 27. *Section 26, problems 4.*
Give addition and multiplication tables for $2\mathbb{Z}/8\mathbb{Z}$. *Are* $2\mathbb{Z}/8\mathbb{Z}$ *and* $\mathbb{Z}_4$ *isomorphic rings?*

$+$	$0+8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$,	$6+8\mathbb{Z}$
$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$
$2+8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$	$0+8\mathbb{Z}$
$4+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$	$0+8\mathbb{Z}$	$2+8\mathbb{Z}$
$6+8\mathbb{Z}$	$6+8\mathbb{Z}$	$0+8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$

$\cdot$	$0+8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$,	$6+8\mathbb{Z}$
$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$
$2+8\mathbb{Z}$	$0+8\mathbb{Z}$	$4+8\mathbb{Z}$	$0+8\mathbb{Z}$	$4+8\mathbb{Z}$
$4+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$
$6+8\mathbb{Z}$	$0+8\mathbb{Z}$	$4+8\mathbb{Z}$	$0+8\mathbb{Z}$	$4+8\mathbb{Z}$

Not isomorphic rings. Z_4 *has unity but* $2\mathbb{Z}/8\mathbb{Z}$ *does not.*

Problem 28. *Section 26, problems 17.*
Let $R = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ *and let* R' *consist of all* 2×2 *matrices of the form* $\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$ *for* $a, b \in \mathbb{Z}$. *Show that* R *is a subring of* $\mathbb{R}$ *and that* R' *is a subring of* $M_2(\mathbb{Z})$. *Then show that* $\phi : R \to R'$, *where* $\phi(a + b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$ *is an isomorphism.*

$k_1 = a_1 + b_1\sqrt{2} \in R, k_2 = a_2 + b_2\sqrt{2} \in R, a_1, a_2, b_1, b_2 \in \mathbb{R}$

(1) $0_{\mathbb{R}} = 0 + 0\sqrt{2} \in R$
(2) $k_1 + k_2 = (a_1 = a_2) + (b_1 + b_2)\sqrt{2} \in R$
(3) $-k_1 = (-a_1) + (-b)\sqrt{2} \in R$
(4) $k_1k_2 = a_1a_2 + (a_1b_2 + a_2b_1)\sqrt{2} + 2b_1b_2 = (a_1a_2 + 2b_2b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$

$k_1 = \begin{pmatrix} a_1 & 2b_1 \\ b_1 & a_1 \end{pmatrix} \in R, k_2 = \begin{pmatrix} a_2 & 2b_2 \\ b_2 & a_2 \end{pmatrix} \in \mathbb{Z}$

(1) $0_{\mathbb{M}_2(\mathbb{Z})} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R'$
(2) $k_1 + k_1 = \begin{pmatrix} a_1 + a_2 & 2(b_1 + b_2) \\ b_1 + b_2 & a_1 + a_2 \end{pmatrix} \in R'$
(3) $-k_1 = \begin{pmatrix} -a_1 & -2b_1 \\ -b_1 & -a_1 \end{pmatrix} \in R'$

(4) $k_1k_2 = \begin{pmatrix} a_1a_2 + 2b_1b_2 & 2a_1b_2 + 2b_1a_2 \\ b_1a_2 + a_1b_2 & 2b_1b_2 + a_1a_2 \end{pmatrix} \in R'$

Injective, surjective.

$$\phi(a_1 + b_1\sqrt{2})\phi(a_2 + b_2\sqrt{2}) = \begin{pmatrix} a_1a_2 + 2b_1b_2 & 2a_1b_2 + 2b_1a_2 \\ b_1a_2 + a_1b_2 & 2b_1b_2 + a_1a_2 \end{pmatrix}$$

$$\begin{aligned} \phi((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) &= \phi((a_1a_2 + 2b_2b_2) + (a_1b_2 + a_2b_1)\sqrt{2}) \\ &= \begin{pmatrix} (a_1a_2 + 2b_2b_2) & 2(a_1b_2 + a_2b_1) \\ (a_1b_2 + a_2b_1) & (a_1a_2 + 2b_2b_2) \end{pmatrix} \end{aligned}$$

$= \phi(a_1 + b_1\sqrt{2})\phi(a_2 + b_2\sqrt{2})$.

Problem 29. *Section 26, problems 18. Show that each homomorphism from a field to a ring is either one to one or maps everything onto 0. Kernel of a homomorphism is an ideal.*
According to our theorems, in any field F, the only ideals can be F or $\{0\}$.
$ker(f) = \{0\}$, it is one-to-one.
$ker(f) = F, \forall x \in F, f(x) = 0$, maps everything to 0.

Problem 30. *"'(Canonical projection)"' Suppose I is an ideal of a ring R. Define a map $\pi : R \to R/I$ by the formula $\pi(r) = r + I$. Show that π is an epimorphism, and that it is a unital epimorphism whenever R is a unital ring.*

$$\begin{aligned} \pi(r_1 + r_2) &= r_1 + r_2 + I \\ &= (r_1 + I) + (r_2 + I) \\ &= \pi(r_1)\pi(r_2) \\ \pi(r_1r_2) &= r_1r_2 + I \\ \pi(r_1)\pi(r_2) &= (r_1 + I)(r_2 + I) \\ &= r_1r_2 + (r_1 + r_2)I + I^2 \end{aligned}$$

anything with I is in I

$$\begin{aligned} \pi(r_1)\pi(r_2) &= r_1r_2 + I \\ \pi(r_1r_2) &= \pi(r_1)\pi(r_2) \end{aligned}$$

It is surjective, therefore epimorphism.

Problem 31. *Let $\pi : R \to R/I$ be the canonical projection defined above. Calculate* $\ker(\pi)$.

$$\begin{aligned} \pi(r) &= 0_{R/I} \\ r + I &= 0_R + I \\ r - 0_R &\in I \\ r &\in I \\ ker(\pi) &= I \end{aligned}$$

Problem 32. *Prove that $R/\{0\}$ is always isomorphic to R itself. "(Hint: use the your calculation of* $\ker(\pi)$ *from the last problem.)"*
$R/\{0\} \backsimeq R$
$\pi : R \to R/\{0\}$ *is always an epimorphism. But* $ker(\pi) = \{0\}$. *So* π *is also a monomorphism.*

Problem 33. *Prove that R/R is always a zero ring. "(Hint: use the equality test for cosets.)"*
Check if R/R has a single element.
Choose any two elements $r_1 + R$, $r_2 + R$.

$$\begin{aligned} r_1 - r_2 &\in R \\ r_1 + R &= r_2 + R \end{aligned}$$

R *only contains one element, which is* 0. R *is a zero string.*

Problem 34. *We shall see next week that there is one and only one ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_3$ for which $\phi(1) = (1, 1)$. Write the table of values for this homomorphism, then describe* $\mathrm{im}(\phi)$ *and* $\ker(\phi)$.

x	$\phi(x)$
0	$(0, 0)$
1	$(1, 1)$
2	$(0, 2)$
3	$(1, 0)$
4	$(0, 1)$
5	$(1, 2)$

$im(\phi) = \mathbb{Z}_2 \times \mathbb{Z}_3; ker(\phi) = 6\mathbb{Z}$

Problem 35. *Repeat the above exercise with $\mathbb{Z}_2 \times \mathbb{Z}_4$ in place of $\mathbb{Z}_2 \times \mathbb{Z}_3$.*

x	$\phi(x)$
0	$(0, 0)$
1	$(1, 1)$
2	$(0, 2)$
3	$(1, 3)$
4	$(0, 0)$

$im(\phi) = \mathbb{Z}_2 \times \mathbb{Z}_4; ker(\phi) = 4\mathbb{Z}$

Problem 36. *By comparing the previous two exercises, see whether you can make any conjecture about the relationship between* $\mathbb{Z}_a \times \mathbb{Z}_b$ *and* $\mathbb{Z}_{ab}$*. (If you manage this then you will have re-discovered the ancient and beautiful "Chinese Remainder Theorem" (CRT), which we will study next week.)*

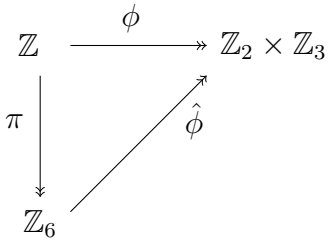
$\mathbb{Z}_a \times \mathbb{Z}_b \backsimeq \mathbb{Z}_{ab}$ *iff* $gcd(a, b) = 1$.
$\mathbb{Z}_{\frac{ab}{gcd(a,b)}}$ *is isomorphic to prime elements of* $\mathbb{Z}_a \times \mathbb{Z}_b$.

5. Week5

5.1. **Definitions(A5).** ▶ **The "initial morphism" from $\mathbb{Z}$ to any unital ring R**: let R be any unital ring. Then there exists one and only one unital morphism $\iota : \mathbb{Z} \to R$. We call this ι the initial morphism into R.
Example:
Compute the initial morphism $\iota : \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_3$.

x	$\phi(x)$
0	$(0,0)$
1	$(1,1)$
2	$(0,2)$
3	$(1,0)$
4	$(0,1)$
5	$(1,2)$

In this case, $im(\iota) = \mathbb{Z}_2 \times \mathbb{Z}_3$; $ker(\iota) = 6\mathbb{Z}$.



▶ **char(R)** (the "characteristic" of a unital ring R): Kernel: this is less predictable. All we know in general is that this is an ideal of $\mathbb{Z}$. But every ideal of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some unique non-negative generator n. This unique non-negative generator for $ker(\iota)$ is called the characteristic of R, denoted **char R**.
Example:
Calculate char $\mathbb{Z}_3$.

x	$\iota(x)$
-1	$[2]$
$\cdots$	$\cdots$
0	$[0]$
1	$[1]$
2	$[2]$
3	$[0]$
4	$[1]$
5	$[2]$
$\cdots$	$\cdots$

$\iota(3) = \iota(1) + \iota(2)$; char $\mathbb{Z}_3 = 3$; In general, char $\mathbb{Z}_n = n$.

▶ **The "prime subring" of a unital ring R**: Suppose R is any unital ring. The **prime subring** of R is the subring generated by 1_R. This is the smallest unital subring.
Example:
$R = \mathbb{Q}$

$$\left\langle \{\frac{1}{1}\} \right\rangle = \{\cdots, -\frac{1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{2}{1}, \cdots\} = \mathbb{Z}$$

▶ **Zero-divisor** (in a commutative ring R): Let R be a ring, and $a \in R$. We say that a is a **left zero-divisor** (may not be commutative) if

(1) $a \neq 0$, and
(2) $\exists b \in R$, with $b \neq 0$ but $ab = 0$.

▶ **Integral domain**: An **integral domain** is a commutative, unital ring, not the zero ring, which has no zero-divisor.
Example:
$\mathbb{Z}_5$ has no zero-divisor.
Find the zero-divisors in $\mathbb{Z}_5$:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

There is no zero-divisor according to the table. $\mathbb{Z}_5$ is an integral domain; $\mathbb{Z}_6$ is not an integral domain.

▶ **Field**: A **field** is a commutative, unital ring, not the zero ring, in which every non-zero element is a unit.
Example:

$$\mathbb{Q}$$
$$1_{\mathbb{Q}} = \frac{1}{1}$$
$$(\frac{a}{b})^{-1} = \frac{b}{a}$$
$$\mathbb{R}, \mathbb{C}$$

5.2. **Theorems (A5). ★ Theorem relating the prime subring to the characteristic** (i.e. "The prime subring of a unital ring R is an isomorphic copy of..."): The prime subring of a unital ring R is an isomorphic copy of the smallest unital subring

★ **Formula for** $\text{char}(\mathbb{Z}_{\mathbf{a}} \times \mathbb{Z}_{\mathbf{b}})$: $\text{char}(\mathbb{Z}_a \times \mathbb{Z}_b) = \text{char}(\mathbb{Z}_{lcm(a,b)})$

★ **Chinese Remainder Theorem**: $\mathbb{Z}_a \times \mathbb{Z}_b$ is isomorphic to $\mathbb{Z}_{ab}$ iff $gcd(a, b) = 1$.

★ **Theorem concerning the characteristic of an integral domain**:

(1) **Zero-Product Property**
If D is an **integral domain**, and $a, b \in D$ with $ab = 0$, then either $a = 0$ or $b = 0$.

(2) **Cancellation Law**
Suppose D is a integral domain, $a \neq 0$, and $ab = ac$. Then $b = c$.

5.3. **Definition (A6).** ▶ Euler totient function (as examples please give one or two illustrative calculations of its values; non-examples are not sensible or needed in this case): The **Euler Totient** is the function

$$\phi : \mathbb{Z}_{>0} \to \mathbb{Z} \text{defined by}$$
$$\phi(n) = |U(\mathbb{Z}_n)|$$
$$\phi(p) = p - 1$$

5.4. **Theorem (A6).** ★ Theorem characterizing the units of $\mathbb{Z}_n$ (i.e. $[a] \in \mathbb{Z}_n$ is a unit if and only if...): $[a] \in \mathbb{Z}_n$ is a unit if and only if a is a coprime to n

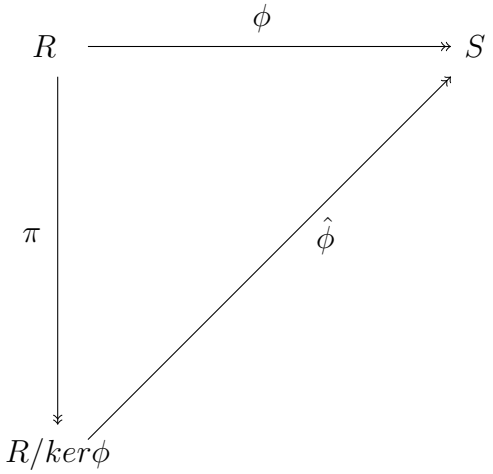
★ Formula for $\phi(p^k)$ when p is prime:$\phi(p^k) = p^k - p^{k-1}$

★ Formula for $\phi(ab)$ when $\gcd(a, b) = 1$: $\phi(ab) = \phi(a)\phi(b)$

★ Formula for $\phi(n)$ when the prime factorization $n = p_1^{k_1} \dots p_l^{k_l}$ is known: $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$

5.5. FTH: Foundamental Theorem of Homomorphism.

Theorem 18. ***FTH: Foundamental Theorem of Homomorphism***
Suppose $\phi : R \to S$ is a ring morphism. Let $\pi : R \to R/ker\phi$ be canonical projection. Then $\exists!monomorphism\hat{\phi} : R/ker\phi \to S$ such that $\hat{phi} \circ \pi = \phi$. (!: unique).



Proof. R, S and $R/ker\phi$ are all groups under $+$. And ϕ is a group morphism. Apply group theory FTH. We get unique group monomorphism $\hat{\phi}$ with $\hat{\phi} \circ \pi = \phi$.

$$\hat{\phi}(r + ker(\phi) = \phi(r)$$
$$\text{Now check :}$$
$$\hat{\phi}((r_1 + ker(\phi)(r_2 + ker(\phi) = \hat{\phi}(r_1 r_2 + ker(\phi)) = \phi(r_1 r_2)$$
$$\text{OTOH,}$$
$$\hat{\phi}(r_1 + ker(\phi))\hat{\phi}(r_2 + ker(\phi)) = \phi(r_1)\phi(r_2)$$

These are equal because ϕ is a ring morphism. □

5.6. The initial morphism and the characteristic of a unital ring.

Definition 25. ***Equalizer***
Suppose $\phi : R \to S$ and $\psi : R \to S$ are both morphisms. The ***equalizer*** *of ϕ and ψ is the set of inputs where ϕ and ψ agree: $Eq(\phi, \psi) = \{r \in R | \phi(r) = \psi(r)\}$.*

Lemma 1. *$Eq(\phi, \psi)$is a substring of R*

Proof.

$$\begin{aligned} \phi(0_R) &= 0_S \\ \psi(0_R) &= 0_S \\ 0_R &\in Eq(\phi, \psi) \end{aligned}$$

$$\begin{aligned} \text{now suppose } r \in Eq(\phi, \psi) & \\ \text{Then } \phi(-1) &= -\phi(r) \\ \psi(-r) &= -\psi(r) \\ \text{so } -r &\in Eq(\phi, \psi) \end{aligned}$$

Suppose $r_1, r_2 \in Eq(\phi, \psi)$.

$$\begin{aligned} \phi(r_1 + r_2) &= \phi(r_1) + \phi(r_2) \\ &= \psi(r_1) + \psi(r_2) \\ &= \psi(r_1 + r_2) \\ \text{so } r_1 + r_2 &\in Eq(\phi, \psi) \end{aligned}$$

Suppose $r_1, r_2 \in Eq(\phi, \psi)$.

$$\begin{aligned} \phi(r_1 r_2) &= \phi(r_1)\phi(r_2) \\ &= \psi(r_1)\psi(r_2) \\ &= \psi(r_1 r_2) \\ \text{so } r_1 r_2 &\in Eq(\phi, \psi) \end{aligned}$$

□

Definition 26. ***initial morphism***
let R be any unital ring. Then there exists one and only one unital morphism $\iota : \mathbb{Z} \to R$. We call this ι the initial morphism into R.

Proof. (Uniqueness)
Suppose $\iota_1 : \mathbb{Z} \to R$ and $\iota_2 : \mathbb{Z} \to R$ are both unital morphisms.
Then $Eq(\iota_1, \iota_2)$ is a subring of $\mathbb{Z}$. It contains 1 because ι_1, ι_2 are both unital. Thus $Eq(\iota_1, \iota_2) = \mathbb{Z}$ so $\iota_1 = \iota_2$.
(Existence)
Define

$$\begin{aligned} \iota(n) &= n \cdot 1_R \text{ (nth multiple of } 1_R) \\ \iota(n_1 + n_2) &= (n_1 + n_2)1_R \\ &= n_1 1_R + n_2 1_R \text{ (laws of multiples)} \end{aligned}$$

x	$\iota(x)$
$\cdots$	$\cdots$
-1	-1_R
0	0_R
1	1_R
2	$1_R + 1_R$
3	$1_R + 1_R + 1_R$
$\cdots$	$\cdots$

Sketch of proof for multiplication:

$$\phi(n \cdot m) = 1_R + 1_R + \cdots + 1_R (nm \text{ times})$$

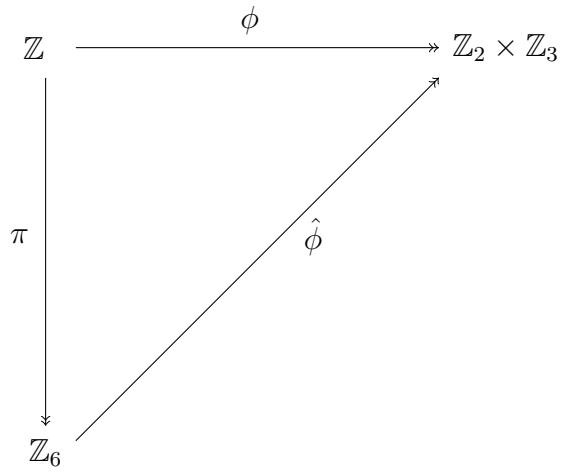
$$\begin{aligned} \iota(n)\iota(m) &= (1_R + \cdots + 1_R)(1_R + \cdots + 1_R) \text{ (n and m times)} \\ &= 1_R + \cdots + 1_R \text{ (nm times)} \end{aligned}$$

□

Example 24. *Compute the initial morphism $\iota : \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_3$.*

x	$\phi(x)$
0	$(0,0)$
1	$(1,1)$
2	$(0,2)$
3	$(1,0)$
4	$(0,1)$
5	$(1,2)$

In this case, $im(\iota) = \mathbb{Z}_2 \times \mathbb{Z}_3$.
$ker(\iota) = 6\mathbb{Z}$.



5.7. **Characteristic of a unital ring, Chinese Remainder Theorem (Sun-Tzu).** What are the image and kernel of ι?
Image: $\iota[\mathbb{Z}] = n \circ 1_R$. This is the prime subring of R.

Kernel: this is less predictable. All we know in general is that this is an ideal of $\mathbb{Z}$. But every ideal of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some unique non-negative generator n.
This unique non-negative generator for $ker(\iota)$ is called the characteristic of R, denoted **char R**.

Example 25. *Calculate char* $\mathbb{Z}_3$.

x	$\iota(x)$
-1	$[2]$
$\cdots$	$\cdots$
0	$[0]$
1	$[1]$
2	$[2]$
3	$[0]$
4	$[1]$
5	$[2]$
$\cdots$	$\cdots$

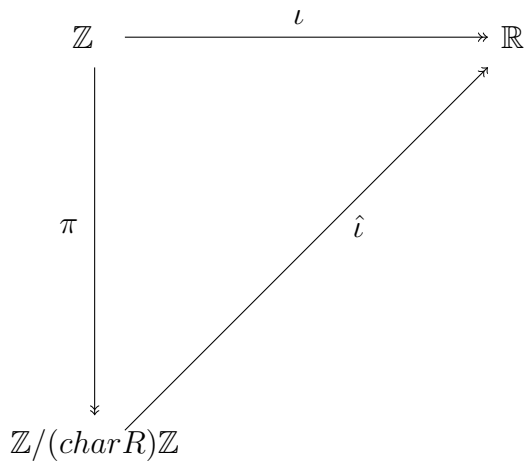
$\iota(3) = \iota(1) + \iota(2)$
char $\mathbb{Z}_3 = 3$
In general, char $\mathbb{Z}_n = n$.

Example 26. *char* $\mathbb{R}$.

x	$\iota(x)$
$\cdots$	$\cdots$
-1	$-1.000000\cdots$
0	$0.000000\cdots$
1	$1.000000\cdots$
2	$2.000000\cdots$
3	$3.000000\cdots$
4	$4.000000\cdots$
5	$5.000000\cdots$
$\cdots$	$\cdots$

$ker(\iota) = 0\mathbb{Z}$
char $\mathbb{R} = 0$

Now er apply FTH:



$\hat{\iota}$ is a monomorphism.So if we restrict its codomain to the actual image, we get an isomorphism:

$$\hat{\iota}\mathbb{Z}/(charR)\mathbb{Z} \to (\text{ prime subring of } R)$$

Corollary 3. *Prime subring of $\mathbb{Z}_a \times \mathbb{Z}_b$ is isomorphic to $\mathbb{Z}_{lcm(a,b)}$.*

5.8. **Chinese Remainder Theorem.** $\mathbb{Z}_a \times \mathbb{Z}_b$ is isomorphic to $\mathbb{Z}_{ab}$ iff $gcd(a,b) = 1$.

Proof. Suppose $gcd(a,b) = 1$
Then $lcm(a,b) = \frac{ab}{gcd(a,b)} = ab$.
So prime subring is isomorphic to $\mathbb{Z}_{ab}$. But subring is all of $\mathbb{Z}_a \times \mathbb{Z}_b$.
OTOH, suppose $gcd(a,b) > 1$. Then the prime subring of $\mathbb{Z}_a \times \mathbb{Z}_b$ is $\mathbb{Z}_{ab}/gcd(a,b)$. So it is a proper subring of $\mathbb{Z}_a \times \mathbb{Z}_b$.

□

5.9. **The Euler Totient Function.**

Definition 27. *The **Euler Totient** is the function*

$$\phi : \mathbb{Z}_{>0} \to \mathbb{Z} \text{defined by}$$
$$\phi(n) = |U(\mathbb{Z}_n)|$$

Table on small values.

$$\phi(1) = |U(\mathbb{Z}_1) = \{0\}| = 1$$
$$\phi(2) = |U(\mathbb{Z}_2) = \{1\}| = 1$$

(Look between 1 and n which are coprime to n)

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
1	1
7	6
$\cdots$	$\cdots$

$\phi(p) = p - 1$

Some better computational mthods:

(1) $\phi(p) = p - 1$
(2) $\phi(p^k) = p^k - p^{k-1}$
(3) If $gcd(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$

Proof.

$$\begin{aligned} \mathbb{Z}_{ab} &\simeq \mathbb{Z}_a \times \mathbb{Z}_b \\ |U(\mathbb{Z}_{200})| &\simeq |U(\mathbb{Z}_8 \times \mathbb{Z}_{25})| \\ &\simeq |U(\mathbb{Z}_8)| \times |U(\mathbb{Z}_{25}| \end{aligned}$$

□

(4) $\phi(p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}) = \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_l^{k_l})$

Clever use of Chinese Reminder Theorem:

$$\mathbb{Z}_8 \times \mathbb{Z}_{25} \simeq \mathbb{Z}_{200}$$

$$|U(\mathbb{Z}_{200})| \simeq |U(\mathbb{Z}_8 \times \mathbb{Z}_{25})| \simeq |U(\mathbb{Z}_8)| \times |U(\mathbb{Z}_{25}|$$

Note: *gcd* has to be 1.

Example 27. (1) $\phi(7) = 7 - 1 = 6$
(2) $\phi(30) = \phi(2)\phi(3)\phi(5) = 1 \cdot 2 \cdot 4 = 8$

Basic principle: Calculating the totient is easy once you know the prime factorization of the input.
But finding prime factorizations of really large numbers is really hard, even for nation-states.
Maybe there is some clever way to compute ϕ without doing prime factorization? BUT NO!

5.10. **A5 Problems.**

Problem 37. *Section 18, problems 15.*
Unit of $\mathbb{Z} \times \mathbb{Z} = (1,1), (-1,1), (1,-1), (-1,-1)$

Problem 38. *Section 18, problems 17.*
All non-zero elements of $\mathbb{Q}$ *are units.*

Problem 39. *Section 18, problems 18.*
$(1,q,1), (1,q,-1), (-1,q,1), (-1,q,1)$. *q as problem 17.*

Problem 40. *Section 18, problems 40.*
$\phi(2) = +3|| - 3, \phi(2n) = 3n| \ -3n$
$\phi(4) = 6|| - 6$, *however,* $\phi(2)\phi(2) = 3^2 = 9$.

Problem 41. *Section 19, problems 1.*
$0, 3, 5, 8, 9, 11$

Problem 42. *Section 19, problems 2.*
3*;* 16 *(Euclidean Algorithm)*

Problem 43. *Section 19, problems 5.*
0

Problem 44. *Section 19, problems 7.*
0

Problem 45. *Section 19, problems 9.*
12

Problem 46. *Section 19, problems 11.*

$$a^4 + 2a^2b^2 + b^4$$

Problem 47. *(The Freshman's Dream) Suppose that* R *is a commutative, unital ring of characteristic two, and choose any* $a, b \in R$. *Prove that* $(a+b)^2 = a^2 + b^2$. *"(Please do not reveal this theorem to actual freshmen, who must work in rings of characteristic zero and who already have enough trouble squaring binomials correctly.)"*

$$(a+b)(a+b) = a^2 + 2ab + b^2$$
$$2ab = 2 \cdot 1 \cdot ab = 0$$
$$(a+b)(a+b) = a^2 + b^2$$

Problem 48. *(The Freshman's Dream in general) Generalize the above exercise as follows: let* R *be a commutative, unital ring of prime characteristic* p, *and let* $a, b \in R$ *be arbitrary. Prove that* $(a+b)^p = a^p + b^p$.

"(Hint: use the Binomial theorem binomial theorem, which is valid in any commutative ring.)"

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k}y^k$$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p\cdot(p-1)!}{k!(p-k)!}$$

p is a prime:

$$\frac{p\cdot(p-1)!}{k!(p-k)!} = p\cdot(\frac{(p-1)!}{k!(p-k)!})$$

Except from $k=1, k=p$, *all* $\frac{(p-1)!}{k!(p-k)!} \in \mathbb{Z}$, $p\cdot(\frac{(p-1)!}{k!(p-k)!}) = 0$

$k=1, k=p$, $\binom{p}{k} = 1$. $(x+y)^p = x^p + y^p$

Problem 49. *Give an example to show that the Freshman's Dream does "not" hold in composite characteristic.*

$(x+y)^4 = x^4+4x^3y+6x^2y^2+4xy^3+y^4 = x^4+4x^3y+4x^2y^2+2x^2y^2+4xy^3+y^4$

$$= x^4 + 2x^2y^2 + y^4$$

Problem 50. *Suppose that R is a commutative, unital ring, and that $a \in R$ is a unit. Show that a is "not" a zero-divisor. "(Hint: suppose to the contrary that there exists $b \neq 0$ with $ab = 0$. What happens if you multiply this equation by a^{-1}?)"*

Assume a is a zero divisor.

$$\exists k \in R, ak = 0$$

$$a^{-1}ak = a^{-1}0$$

$$1_R k = 0$$

However,

$$1_R k = k$$

proved by contradiction.

Problem 51. *Prove that every field is an integral domain.*

Field: Every non-zero element is a unit (not zero divisor). Which means it is an integral domain.

Problem 52. *Generalize the above result by showing that any unital subring of a field is an integral domain. "(Hint: Suppose that F is a field and R is a unital subring of F. If R had zero-divisors, then they would also be zero-divisors in F.)"*

Suppose F is a field and R is a unital subring of F.

Assume R is not an integral domain and has zero-divisor, then F will

have element which is a zero divisor. However, all non-zero elements should be unit and should not be zero-divisor. All unital subrings combined to be F. F should be an integral domain.

Problem 53. *Suppose that D is an integral domain. Show that* $\mathrm{char}(D)$ *is either zero or a prime. "(Hint: suppose to the contrary that* $\mathrm{char}(D)$ *is composite, say* $\mathrm{char}(D) = nm$ *for* $n, m > 1$ *and let* ι *be the initial morphism. What is* $\iota(n) \cdot \iota(m)$*?)"*
Assume

$$char(D) = mn$$
$$char(D) \cdot 1_R = 0$$
$$mn \cdot 1_R = 0$$
$$mn = 0$$

m, n are zero divisors. D cannot be an integral domain.

5.11. **A6 Problems.**

Problem 54. *Make a table showing the values of* $\phi(n)$ *for* $n \in \{1, 2, 3, \ldots, 20\}$.

n	$\phi(n)$
1	*0*
2	*1*
3	*2*
4	*2*
5	*5*
6	*2*
7	*6*
n	$(p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdots$

Problem 55. *Two students try to calculate* $\phi(45)$ *as follows: one says that* $\phi(45) = \phi(9)\phi(5) = (3^2 - 3^1)(5-1) = 6 \times 4 = 24$*, and another says that* $\phi(45) = \phi(3)\phi(15) = \phi(3)\phi(3)\phi(5) = (3-1)(3-1)(5-1) = 16$*. Which one is wrong, and why?*
Second one is wrong. $(3-1)(3-1)$ *is calculating all combinations of* 1 *and* 2*, ignoring everything which is relative prime to 2 and 3. Wrong counting.*

Problem 56. *The table you constructed above should show that* $\phi(15) = 8$*. Working in* $\mathbb{Z}_{15}$*, compute the following expressions:* $1^8, 2^8, 4^8, 7^8, 8^8, 11^8, 13^8$*, and* 14^8*. "(Hint: there are various tricks that make these computations easier than they look. For example, when computing powers of* 4 *you will quickly find that* $4^2 = 16 = 1$*, from which it follows that* $4^8 = (4^2)^4 = 1^4 = 1$*. For another example, when computing powers of* 14 *it will help to notice that* $14 = -1$*. Using tricks like this, a clever person can compute all of these expressions with very little work.)"*
All 1

Problem 57. *Based on the previous problem, try to formulate a conjecture regarding the value of the expression* $a^{\phi(n)}$ *in* $\mathbb{Z}_n$*.*
1, if $gcd(a, n) = 1$

Problem 58. *Try to prove the conjecture you formulated above. "(Hint: Lagrange's Theorem is very, very helpful.)"*
$\phi(n)$ *elements in the cyclic group.* $g^{|G|(=\phi(n))} = 1$

Problem 59. *Again working in* $\mathbb{Z}_{15}$*, compute the expressions* $3^8, 5^8, 6^8, 9^8, 10^8$*, and* 12^8*. Do these contradict the conjecture you formulated above? (If so, then reformulate the conjecture. If your initial conjecture was wrong, then reformulating it may give you a crucial hint about how to prove the reformulated conjecture, since any successful proof will need*

to make some use of the additional hypothesis. The process of mathematical discovery often works this way—it is good to learn from one's mistakes.)

$$\{3, 6, 9, 12\}$$
$$\{5, 10\}$$
$3^5 = 3,\ 6^5 = 6 \cdots\ 3^8 = 3 \cdots 3^3 = 6,\ 6^8 = 6 \cdot 6^3 = 6. \cdots$

6. **Week6**

6.1. **Definitions.** ▶ Private key (in the RSA cryptosystem; i.e. "The private key is the ordered pair consisting of..."): The private key is the ordered pair (N, d)consisting of $N = pq$ and $d = e^{-1} \in \mathbb{Z}_{\phi(N)}$, where $gcd(e, \phi(N)) = 1$

▶ Public key (in the RSA cryptosystem). The public key is the ordered pair (N, e)consisting of $N = pq$ and e, where $gcd(e, \phi(N)) = 1$

▶ Formal fraction (from an integral domain D): A formal fraction from D is a member of $D \times (S - \{0\})$.

▶ Equivalence (of formal fractions): Define a binary relation on $D \times (D - \{c\})$ as follows: $(a, b) \sim (c, d) \iff ad == bc$.

▶ Fraction (from an integral domain D): A fraction is a $\sim$ equivalence class of formal fraction.

▶ Frac(D) (the "field of fractions" of the integral domain D): The collection of all fractions from D is denoted $Frac(D)$.

6.2. **Theorems.** ★ Euler's Theorem: Suppose a, n are positive integers with $gcd(a, n) = 1$. Then

$$a^{\phi(n)} \equiv_n 1$$

★ Equality test for fractions:

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc$$

Last time: Euler totient function:

$$\phi(n) = |U(\mathbb{Z}_n)|$$

Today: Euler's Theorem
Intro to cryptosystem

6.3. **Euler's Theorem.**

Theorem 19. *(Euler)*
Suppose a, n are positive integers with $gcd(a, n) = 1$. Then

$$a^{\phi(n)} \equiv_n 1$$

Proof. First, recall the following corollary of Lagrange's Theorem: If G is any finite group, and $a \in G$, then $a^{|G|} = e$.
Now, because $gcd(a, n) = 1$, we have $[a] \in U(\mathbb{Z}_n)$. So in $U(\mathbb{Z}_n)$, we have

$$[a]^{\phi(n)} = [1]$$
$$[a^{\phi(n)}] = [1]$$

so $a^{\phi(n)} \equiv_n 1$.

□

6.4. **Mathematical structure of cryptosystems.** Problem: We need to send a message (plaintext) to a defined list of recipients. No one else should be able to read the message, even if it is intercepted. So we will transform it into a "ciphertext", which will look like nonsense to "adversaries".

Example 28. *The Caesar Cipher.*
ATTACK THE LEFT FIANK2 → (Shift everything by 3).
DWWDFN · · ·

(1) Plaintext is "encoded" as a sequence of elements of some group G (here $G = \mathbb{Z}_{26}$)
(2) The group G is called the "site" of the cryptosystem.
(3) There is a key known to the sender but not the adversary (here $k = 3$) that is used to define an invertible encryption map $E : G \to G$ (here $E(x) = x + k$)
Applying this element by element to plaintext gives ciphertext.
(4) There is another key (here -3) known to the recipient, which can be used to compute a decryption map $D : G \to G$, with D, E inverse function.

Two types of cryptosystem:

(1) Symmetric. Anyone who knows the encryption key can easily figure out the decryption key.
(2) Asymmetric (Not symmetric): someone who can encrypt does not easily know how to decrypt.

Key distribution problem:
In any symmetric system, both parties must possess the key before communication begins. How did this happen?
WHY DIDN'T THE ADVERSARY INTERCEPT THE KEY?

Unbreakable code during world war 2:
VOTP - actually unbreakable symmetric cipher.
(Fast exponentiation: exp. by repeated squarings.

Lats time: cryptosystems and the key distribution problem.

6.5. **RSA Encryption.** (1970s, Rivest, Shamir, Adelmann) - Asymmetric cryptosystem.

$$a^{\phi(n)} \equiv_n 1$$

The players:
Alice - wants to receive secure comms.
Bob - wants to send a message to Alice.
Eve - wants to eavesdrop.
Process:

(1) Key Generation
(2) Encryption
(3) Decryption

(1) RSA key generation (ssh-keygen) - Done by Alice
    (a) Alice chooses two very large primes p, q
        - unpredictability of p, q is essential to security.
    (b) Alice sets $N = pq$
    (c) Alice computes $\phi(N) = \phi(pq) = (p-1)(q-1)$
    (d) Alice chooses encryption exponent e with $gcd(e, \phi(N)) = 1$.
    (e) e is a unit of $\mathbb{Z}_{\phi(N)}$. Alice computes $d = e^{-1}$ (in the ring $\mathbb{Z}_{\phi(N)}$) (d is decryption exponent).

(f) The pair (N, e) is the public key. Alice broadcasts this to the world.
The pair (N, d) is the private key. This is kept secret.

(2) Encryption.
(a) Bob "encodes" his message as an element of $\mathbb{Z}_N$. Call this m (plaintext).
(b) Bob computes $c = m^e$ (in $\mathbb{Z}_N$). c is the ciphertext. Bob transmits c.

(3) Decryption
(a) Alice receives c. She computes:

$$c^d$$

We shall show that c^d coincides with m.

Proof. in $\mathbb{Z}_{\phi(N)}$, $d = e^{-1}$, so:
in $\mathbb{Z}_{\phi(N)}$, $[de] = [1]$. $de \equiv_{\phi(N)} 1$
$de - 1$ is a multiple of $\phi(N)$, say

$$de - 1 = k\phi(N)$$
$$de = 1 + k\phi(N)$$

in $\mathbb{Z}_N$

$$\begin{aligned} c^d &= (m^e)^d \\ &= m^{de} \\ &= m^{1+k\phi(N)} \\ &= m \cdot (m^{\phi(N)})^k \\ &= m \cdot 1^k \\ &= m(\text{ provided that } gcd(m, N) = 1) \end{aligned}$$

□

(b) If Eve knew d, she could easily decrypt $d = e^{-1}(mod\phi(N))$, Eve needs $\phi(N)$ to compute this.
$\phi(N) = (p-1)(q-1)$. Finding $phi(N)$ is equivalent to factoring N. This is hard.
Note: $gcd(m, N) = 1$ is guaranteed provided that $m < min(p, q)$.

Example 29. ***RSA Example***

- *Key generation (Alice)*

$$p = 3, q = 5$$
$$N = 15$$

$$\phi(N) = \phi(15) = 8$$

Alice choose $e \in U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$.
$e = 7$ *is choosen. Set* $d = e^{-1} (\in \mathbb{Z}_8) = 7^{-1} = 7$
Public Key: $(N, e) = (15m7)$
Public Key : (N, d) = (15, 7)

- *Encryption (Bob)*
  Bob wants to send some plaintext $m = 8$.

$$c = m^e = 8^7 (in \mathbb{Z}_{15})$$
$$8^7 = 2$$

- *Decryption (Alice):*

$$c = 2$$
$$m = c^d = 2^7 = 128 = 8$$

endenumerate

Today: Fractions.

6.6. **Field of Fractions of an Integral integral domain.** 1st try at defining fractions:
A fraction is an element of $D \times D$.
Ex: $(3,5)$ "represents" $\frac{3}{5}$ Problem: $(3,0)$ represents $\frac{3}{0}$
First "fix:" A fraction is an element of $D \times (D - \{c\})$.
Second Problem: $(3,5)$ represents $\frac{3}{5}$, (6, 10) represents $\frac{6}{10}$. $\frac{3}{5} = \frac{6}{10}$, but $(3,5) \neq (6,10)$.

Definition 28. ***Equivalence of elements of*** $D \times (D - \{c\})$
Define a binary relation on $D \times (D - \{c\})$ *as follows:* $(a,b) \sim (c,d) \iff ad == bc$.

Theorem 20. $\sim$ *is an equivalence relation.*

Proof. $(a,b) \sim (a,b)$ because $ab = ba$.
Suppose $((a,b) \sim (c,d)$, then

$$ad = bc$$
$$bc = ad$$
$$cb = da$$
$$(c,d) \sim (a,b)$$

Transtivity: Suppose $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$

$$ad = bc$$
$$cf = de$$
$$afcd = bcde$$
$$afcd = becd \text{ and } d \neq 0$$

So $afc = bec$ (because we're in an integral domain)
Case 1: $c \neq 0$. Then we cancel it and get $af = be$ and we're done.
Case 2: $c = 0$, then $ad = 0$ and $de = 0$. So $a = 0$ and $e = 0$. Thus $af = 0$ and $be = 0$, so $af = be$.

□

Definition 29. ***Actual Definitions of formal fraction and fraction***
A formal fraction from D *is a member of* $D \times (S - \{0\})$.
A fraction is a $\sim$ *equivalence class of formal fraction.*

Example 30. *The formal fractions* $(3,5)$ *and* $(6,10)$ *are not equal. However, the fractions* $[(3,50]$ *and* $[(6,10)]$ *are equal.* $(3,5) \sim (6,10)$ *because* $3 \cdot 10 = 5 \cdot 6$.

Notation: the fraction$[(a,b)]$ is usually denoted $\frac{a}{b}$. Thus $\frac{3}{5} = \frac{6}{10}$.

Definition 30. ***Equality test for Fractions***

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc$$

The collection of all fractions from D is denoted $Frac(D)$.

Example 31. $Frac(\mathbb{Z}) = \mathbb{Q}$.

Operations on $Frac(D)$:
$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$ ($bd \neq 0$ because $b \neq 0$ and $d \neq 0$ and D is an integral domain)
$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

These turn out to be well-defined. They turn $Frac(D)$ into a ring. In fact $Frac(D)$ is a field.
The zero element of $Frac(D)$ is $\frac{0_D}{1_D} : \frac{a}{b} + \frac{0}{1} = \frac{a\cdot 1 + b\cdot 0}{b\cdot 1} = \frac{a}{b}$

Unity is $\frac{1_D}{1_D} : \frac{a}{b} \cdot \frac{1}{1} = \frac{a\cdot 1}{b\cdot 1} = \frac{a}{b}$.
Inverse of $\frac{a}{b}$ is $\frac{b}{a}$, $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$
Problem: maybe $a = 0$, then

6.7. **Problems.**

Problem 60. *Section 20, problems 5: Use Fermat's theorem to find the remainder of* 37^{49} *when it is divided by* 7.

$$37^6 = 1 \ mod\ 7$$
$$37^{48} = 1^8 = 1 \ mod\ 7$$
$$37^{49} = 1 * 37 = 2 \ mod\ 7$$

Problem 61. *Section 20, problems 10: Use Euler's generalization of Fermat's theorem to find the remainder of* 7^{1000} *when divided by* 24.

$$\phi(24) = (2^3 - 2^2) \times (3 - 1)$$
$$= 4 \times 2 = 8$$
$$7^8 = 1 \ mod\ 24$$
$$7^{1000} = 1^{125} = 1 \ mod\ 24$$

Problem 62. *Taking* $p = 5$ *and* $q = 7$*, generate a public/private key-pair for the RSA cryptosystem. (Hint: start by choosing an encryption exponent* e *which is relatively prime to* $\phi(35) = 24$*. If you have trouble generating the corresponding decryption exponent, use* $e = 5$*, which is easy to invert modulo* 24 *by inspection.*

$$\phi(35) = 4 \times 6 = 24$$
$$e \in \{1, 5, 7, 11, 13, 17, 19, 23\}$$
$$choose\ e = 11$$
$$m^{24} = 1 \ mod\ 35$$
$$m^{ed} = m \ mod\ 35$$
$$ed = 24 \cdot k + 1$$
$$11 \cdot d = 24 \cdot k + 1$$
$$d = 15$$
$$(11, 35); (11, 35)$$

(Euclidean Algorithm for calculating inverse)

Problem 63. *Using the public key generated above, encrypt the "message"* $m = 3$*.*

$$3^4 = 11 \ mod\ 35$$
$$3^8 = 16 \ mod\ 35$$
$$3^{11} = 12 \ mod\ 35$$

Problem 64. *Using the private key generated above, decrypt the "ciphertext" c generated by the previous problem.*

$$12^2 = 4 \ mod \ 35$$
$$12^{10} = 1024 = 9 \ mod \ 35$$
$$12^{11} = 108 = 3 \ mod \ 35$$

Problem 65. *You have undoubtedly noticed that your public and private keys are identical, which is undesirable in an allegedly asymmetric cryptosystem. In fact, for these particular choices of p and q, the two keys will be identical regardless of which encryption exponent is chosen. Try to explain why. "(Hint: investigate the structure of the group* $\mathcal{U}(\mathbb{Z}_{24})$ *using the Chinese Remainder Theorem.)"*

$$U(\mathbb{Z}_{24}) = U(\mathbb{Z}_3 \times \mathbb{Z}_8) = U(\mathbb{Z}_3) \times U(\mathbb{Z}_8)$$

$U(\mathbb{Z}_3).U(\mathbb{Z}_8)$ *are self-inverse.*

Problem 66. *Repeat the previous exercises with slightly larger choices of p and q until you find a keypair in which the keys are distinct. (You may wish to use a machine to help with the arithmetic.)*

$$p = 23, q = 17$$

$$N = 391, \phi(N) = 352$$

Public Key $= (391, 7)$*; Private Key* $= (391, 151)$
Using ***Prime.java***

Generating primes:
Sieve of Eratostheres

Problem 67. *Let D denote the ring of real-valued polynomial functions. (We will see next week that this is an integral domain; for purposes of this problem you may take that fact for granted.) Write down some fractions from D. What did you call objects of this type when you were in high school?*

$$\frac{x^2 + 2x + 1}{x^2 - 1}$$

Problem 68. *With D as above, prove that the fractions* $\frac{x^2-1}{x^2-2x+1}$ *and* $\frac{x+1}{x-1}$ *are equal.*

$$(x^2 - 1, x^2 - x + 1), (x + 1, x - 1)$$

Using the equality test:

$$(x^2-1)(x+1) = x^3 - x^2 - x + 1$$
$$(x^2-2x+1)(x+1) = x^3 + x^2 - 2x^2 - 2x + x + 1 = x^3 - x^2 - x + 1$$
$$(x^2-1)(x+1) = (x^2-2x+1)(x+1)$$
$$\frac{x^2-1}{x^2-2x+1} = \frac{x+1}{x-1}$$

Problem 69. *Suppose that D is any integral domain and that $a, b, c \in D$ with $a \neq 0$ and $b \neq 0$. Prove the "'cancellation property of fractions,"' that $\frac{ab}{ac} = \frac{b}{c}$.*

Problem 70. *Suppose that D is any integral domain and that $a, b, c \in D$ with $b \neq 0$ and a a unit. Prove that $\frac{ab}{c} = \frac{b}{a^{-1}c}$ and that $\frac{b}{ac} = \frac{a^{-1}b}{c}$.*

$$abc = acb$$

Problem 71. *"'(Addition with a common denominator)"' Starting from the definition of addition in* $\mathrm{Frac}(D)$*, show that $\frac{a}{c} + \frac{b}{c} = \frac{a+b}{c}$.*

$$\frac{ac+bc}{c \cdot c}$$
$$(ac+bc) \cdot c = ac \cdot c + bc \cdot c$$
$$c \cdot c \cdot (a+b) = ac \cdot c + bc \cdot c$$

7. **Week7**

7.1. **Definitions.** ▶ Formal fraction (from an integral domain D): A formal fraction from D is a member of $D \times (S - \{0\})$.

▶ Equivalence (of formal fractions):Define a binary relation on $D \times (D - \{c\})$ as follows: $(a, b) \sim (c, d) \iff ad == bc$.

▶ Fraction (from an integral domain D): A fraction is a $\sim$ equivalence class of formal fraction.

▶ Addition (of fractions):$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

▶ Multiplication (of fractions): $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$ ($bd \neq 0$ because $b \neq 0$ and $d \neq 0$ and D is an integral domain)

▶ Frac(D) (the "field of fractions" of the integral domain D): The collection of all fractions from D is denoted $Frac(D)$.

▶ Canonical injection (of an integral domain D into its field of fractions): Define a map $\iota : D \to Frac(D)$ by the formula

$$\iota(a) = \frac{a}{1_D}$$

▶ Polynomial function (from a ring R into itself): Any funtion $f : \mathbb{R} \to \mathbb{R}$ of the form $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ for some fixed constans $a_0, a_1 \cdots a_n$ and some non-negative integer n.

▶ Polynomial expression (with coefficients in a ring R): Let R be any commutative unital ring. A polynomial expression with coeff's in R is a sequence $(a_0, a_1 \cdots)$ of elements of R, which has only finitely many non-zero entries.

▶ Addition (of polynomial expressions): $(a_0, a_1, a_2, \cdots)+(b_0, b_1, b_2, \cdots)$ $= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots)$

▶ Multiplication (of polynomial expressions):

$$(a_0, a_1, a_2) \cdot (b_0, b_1, b_2, \cdots)$$
$$= (c_0, c_1, c_2 \cdots)$$
$$c_k = \sum_{i=0}^{k} a_i b_{k-1} = \sum_{i+j=k} a_i b_j$$

▶ $R[x]$ (the "ring of polynomial expressions, with coefficients in R, in the indeterminate x," or "R adjoin x" for short): $R[x]$ means the set of polynomial expressions w/ coeff's in R. "R adjoin x"

$$R[x] = \{(a_0, a_1, a_2 \cdots) | a_i \in R \text{ and only finitely many } a_i \neq 0\}$$

We could have written $(1, 1, 2, 0, 0, \cdots) = 1 + y + 2y^2$

7.2. **Theorems.** ★ Equality test for fractions:

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc$$

★ Universal mapping property of Frac(D): $Frac(D)$ is a field into which D can be injected. It is in fact the samllest such field, in the following sense: Suppose $\phi : D \to F$ is any monomorphism into any field F. Then ∃! monomorphism $\hat{\phi} : Frac(D) \to F$ making $\hat{\phi} \circ \iota = \phi$. ($\phi$ has to be unital).

★ Example of two distinct polynomial expressions that give rise to the same polynomial function:
Take $R = \mathbb{Z}_3$
Define $f(x) = x^3 + 1 = (1, 1, 0, 0, 0, 0, \cdots)$

x	$f(x)$
0	1
1	2
2	0

$R = \mathbb{Z}_3$

$g(x) = x + 1 = (1, 0, 0, 1, 0, 0, \cdots)$

x	$g(x)$
0	1
1	2
2	0

Notice that $f = g$ over $\mathbb{Z}_3$, $x^3 + 1$ and $x + 1$ are the same polynomial over $\mathbb{Z}_3$.

Last time: $Frac(D)$, field of fractions of D. ($Frac(\mathbb{Z}) = \mathbb{Q}$).

This time: Is D a subset of $Frac(D)$? No. An element of $Frac(D)$ is an equivalence class of pairs of elements of D. But we will now show that D is isomorphic to a certain subring of $Frac(D)$.

7.3. **The canonical injection.**

Definition 31. *Define a map $\iota : D \to Frac(D)$ by the formula*

$$\iota(a) = \frac{a}{1_D}$$

Claim: ι is always a unital monomorphism.

Proof.

$$\iota(a+b) = \frac{a+b}{1}$$
$$\iota(a) + \iota(b) = \frac{a}{1} + \frac{b}{1} = \frac{a+b}{1}$$

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

$a \in ker(\iota) \iff \iota(a) = \frac{0}{1} \iff \frac{a}{1} = \frac{0}{1}$
$\iff a \cdot 1 = 1 \cdot 0 \iff a = 0.$
So $ker(\iota) = \{0\}$ and ι is one-to-one.
Thus, $\iota : D \to Frac(D)$ might not be an isomorphism because it might not be surjective. But if we restrict the codomain to the actual image, it becomes an isomorphism from D to $im(\iota)$.
So $im(\iota)$ is a "copy" of D inside Frac(D).
(double b; int n = (int) b)

So: the integer 5 is not literally the same object as $\frac{5}{1}$. But $\{\frac{n}{1} | n \in \mathbb{Z}\}$ is a "copy of $\mathbb{Z}$ inside $\mathbb{Q}$.

□

What if D was already a field? What will $Frac(D)$ look like?
In this canse $Frac(D)$ will be isomorphic to D.

Proof. $im(D) = \{\frac{a}{1} | a \in D\}$. But any fraction $\frac{a}{b} = \frac{ab^{-1}}{1}$, so $im(\iota)$ is all of $Frac(D)$. □

7.4. **The universal mapping property and concrete models of Frac(D).** Claim: $Frac(D)$ is a field into which D can be injected. It is in fact the samllest such field, in the following sense: Suppose $\phi : D \to F$ is any monomorphism into any field F. Then $\exists!$ monomorphism $\hat{\phi} : Frac(D) \to F$ making $\hat{\phi} \circ \iota = \phi$. ($\phi$ has to be unital).
(Graph)

Proof. Suppose $\hat{\phi}$ is such a monomorphism. Then

$$\begin{aligned}\hat{\phi}(\frac{a}{1}) &= \hat{\phi}(\iota(a)) \\ &= (\hat{\phi} \circ \iota)(a) \\ &= \phi(a)\end{aligned}$$

$$\hat{\phi}(\frac{b}{1} \cdot \frac{1}{b}) = \hat{\phi}(\frac{1}{1}) = \phi(1) = 1_F$$
$$\hat{\phi}(\frac{b}{1}\hat{\phi}(\frac{1}{b}) = 1_F$$
$$\phi(b) \cdot \hat{\phi}(\frac{1}{b} = 1_F \Rightarrow \hat{\phi}(\frac{1}{b}) = (\phi(b))^{-1}$$
$$\begin{aligned}\hat{\phi}(\frac{a}{b}) &= \hat{\phi}(\frac{a}{1})\hat{\phi}(\frac{1}{b}) \\ &= \phi(a)(\phi(b))^{-1}\end{aligned}$$

Existence: Define $\hat{\phi}(\frac{a}{b}) = \phi(a)\phi(b)$.

□

Example 32.

What us $im(\hat{\phi})$ in this case?
Answer: The set of real numbers whose decimal expansion is eventually periodic.
$68135, 214312121212121212121 \cdots$

Example 33. $D = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$
D is a subring of $\mathbb{R}$:
$(2 + 3\sqrt{2}) + (3 - \sqrt{2}) = (5 + 2\sqrt{2})$
$(2 + 3\sqrt{2})(3 - \sqrt{2}) = 69\sqrt{2} - 2\sqrt{2} - 6$
$= 0 + 7\sqrt{2}$
So D is an integral domain.
What does $Frac(D)$ look like?
$\{\frac{a+b\sqrt{2}}{c+d\sqrt{2}} | a, b, c, d \in \mathbb{Z}$ *and either* $c \neq 0$ *or* $d \neq 0\}$

$\frac{7+\sqrt{2}}{6+5\sqrt{2}} \cdot \frac{1+\sqrt{2}}{0+\sqrt{2}} =$

Last time: Universal mapping prop of $Frac(D)$: $im(\hat{\phi})$

7.5. **Polynomials.**

Example 34. *Example:* $f(x) = x^2 + 1$
Non-Example:
$g(x) = \frac{1}{x} = x^{-1}$
$h(x) = \sin(x)$

Correct H.S. definition of "polynomial":

Definition 32. ***polynomial*** *Any funtion* $f : \mathbb{R} \to \mathbb{R}$ *of the form* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *for some fixed constans* $a_0, a_1 \cdots a_n$ *and some non-negative integer* n.

First attempt at generalization: let R be any commutative unital ring. A polynomial function on R is a function $f : R \to R$ of the form $f(x) = a_n x^n + \cdots a_1 x + a_0, (a_0, a_1 \cdots \in R)$.

Example 35. *Take* $R = \mathbb{Z}_3$
Define $f(x) = x^3 + 1$

x	$f(x)$
0	1
1	2
2	0

Example 36. $R = \mathbb{Z}_3$
$g(x) = x + 1$

x	$g(x)$
0	*1*
1	*2*
2	*0*

Notice that $f = g$ over $\mathbb{Z}_3$, $x^3 + 1$ and $x + 1$ are the same polynomial over $\mathbb{Z}_3$.

Next we will define polynomial expression, so that f and g (from prev.) have unequal expressions even though they define the same function.

Definition 33. *Let R be any commutative unital ring. A polynomial expression with coeff's in R is a sequence $(a_0, a_1 \cdots)$ of elements of R, which has only finitely many non-zero entries.*

Example 37. $f(x) = 5x^3+2x-1$ *"encode" this as* $(-1, 2, 0, 5, 0, 0, 0 \cdots)$

Notation: Instead of writing $f = (a_0, a_1, a_2 \cdots)$, we write $f = a_0 + a_1x + a_2x^2 + \cdots$
Question: over $\mathbb{Z}_3$, are the polynomial expressions

$$f(x) = x^3 = +1$$
$$g(x) = x + 1$$

equal? No: $f = (1, 0, 0, 1, 0, 0, \cdots)$; $g = (1, 1, 0, 0, 0, 0, \cdots)$.

Notation: $R[x]$ means the set of polynomial expressions w/ coeff's in R. "R adjoin x"
We could have written $(1, 1, 2, 0, 0, \cdots) = 1 + y + 2y^2$
In this case we would denoted the set of polynomials as $R[y]$.
Binary operations on $R[x]$:
$(a_0, a_1, a_2, \cdots) + (b_0, b_1, b_2, \cdots)$
$= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots)$

Example 38.

$$f(x) = 3 + 4x - 5x^2$$
$$g = 2 + 3x + 0x^2$$
$$f + g = 5 + 7x - 5x^2$$

$0x^2$ *is "zero-pudding"*

Multiplication of polynomials:
$(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x = \cdots + b_nx^n)$
$= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3 + \cdots$

Definition 34. *True Definition of Multiplication:*

$$(a_0, a_1, a_2) \cdot (b_0, b_1, b_2, \cdots)$$
$$= (c_0, c_1, c_2 \cdots)$$
$$c_k = \sum_{i=0}^{k} a_i b_{k-1} = \sum_{i+j=k} a_i b_j$$

Theorem 21. *With these operations, $R[x]$ is again a commutative, unital ring.*

$$0_{R[x]} = 0 + 0x + \cdots$$

$$1_{R[x]} = 1 + 0x + \cdots$$

7.6. **Problems.**

Problem 72. *Section 21, problems 1*
Describe the field F of quotients of the integral subdomain

$$D = \{n + mi | n, m \in \mathbb{Z}\}$$

of $\mathbb{C}$. "Describe" means give the elements of $\mathbb{C}$ that make up the field of quotients of D in $\mathbb{C}$. (The elements of D are the Gaussian integers.)

Problem 73. *Section 21, problems 2*
Describe (in the sense of Exercise 1) the field F of quotients of the integral subdomain $D = \{n + m\sqrt{2} | n, m \in \mathbb{Z}\}$ of $\mathbb{R}$.

Problem 74. $f(x) = 4x - 5, g(x) = 2x^2 - 4x + 2 \in \mathbb{Z}_8[x]$.

$$f(x) + g(x) = 2x^2 - 3 = 2x^2 + 5$$

$$f(x)g(x) = -26x^2 + 28x - 10 = 6x^2 + 4x + 6$$

Problem 75. *How many polynomials are there of degree ≤ 3 in $\mathbb{Z}_2[x]$? (Include 0.)*
$2 \cdot 2 \cdot 2 = 8$

Problem 76. *How many polynomials are there of degree ≤ 2 in $\mathbb{Z}_5[x]$? (Include 0.)*
$5 \cdot 5 = 25$

Problem 77. *(Rational expressions). Next week we shall prove that whenever D is an integral domain, so is $D[x]$. For purposes of this exercise, you may take this fact for granted. Thus, the field of fractions of $D[x]$ is a well-defined object, which is usually denoted $D(x)$. Write down two "random" elements of the field $\mathbb{R}(x)$, and show how to add them, and also how to multiply them.*

$$\frac{1.5x^2 + 3}{x + 1}; \frac{2x^3 - 3.7x + 1}{x^2 - 1}$$

Problem 78. *(An infinite ring with positive characteristic). Let $R = \mathbb{Z}_3[x]$ denote the ring of polynomial expressions with coefficients in $\mathbb{Z}_3$. Write the table of values of the initial morphism $\iota : \mathbb{Z} \to R$, and show*

that $\mathrm{char}(R) = 3$.

x	ι
0	0.000000
1	1.000000
2	2.000000

$char(R) = 0 = 3$

Problem 79. *Let R be as in the previous exercise. Show that R is an infinite ring, even though it has characteristic three and its prime subring is thus a copy of $\mathbb{Z}_3$.*

Problem 80. *Let R be as in the previous exercise and put $F = \mathrm{Frac}(R)$. (We will show next week that R is an integral domain; for purposes of this problem you may take this for granted.) Show that F is an infinite field of positive characteristic.*

(

$$\mathbb{Z}_3[x]$$

has characteristic 3*:*

x	ι
0	0
1	$1 = 0x + \cdots$
2	$2 + 0x + \cdots$
3	$0 \cdots$
4	$1c \ldots$

But $\mathbb{Z}_3[x]$ is an infinite ring: $1, x, x^2, x^3, \cdots$ are all distinct.)

In $F = Frac(\mathbb{Z}_3[x])$

8. **Week8**

8.1. **Definitions.** ▶ Degree (of a polynomial; please be sure to include the case of the zero polynomial): Suppose $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. If $f \neq 0$, then $deg(f)$ means the largest i such that $a_i \neq 0$. By convention, $deg(0) = -\infty$

Example 39.

$$f = 3x - 4x^3 + 25x^4 - x^7 + 0x$$

$deg(f) = 7$

▶ Constant polynomial: A constant polynomial is a polynomial of degree ≤ 0.

▶ Divisibility relation on polynomials: in $D[x], f|g \iff \exists h \in D[x]$ with $g = fh$

▶ $f \,\%\, g$: Given $f, g \in F[x], g \neq 0$, define $f\%g$ to be the remainder when f, is divided by g.
So: $g|f \iff f\%g = 0$

8.2. **Theorems.** ★ Degree bounds on sum and product (general form).

$$deg(f + g) \leq max(deg(f), def(g))$$

$$deg(fg) \leq deg(f) + deg(g)$$

★ Formula for deg(fg) when R is an integral domain.

$$deg(fg) = deg(f) + deg(g) > 0$$

★ Theorem concerning zero-divisors in $D[x]$ when D is an integral domain (i.e. "If D is an integral domain then so is..."): If D is an integral domain, then so is$D[x]$.

★ Theorem on polynomial long division:
Suppose D is an integral domainm and that $f, g \in D[x]$, such that

(1) $g \neq 0$
(2) The leading coefficient of g is a unit of D.

Then $\exists! q, r \in D[x]$ such that

(1) f = gq + r
(2) deg r < deg g

★ Divisibility test for polynomials with coefficients in a field: $f, g \in F[x], g \neq 0$. Let q, r be as in long division. Then $(g|f \iff r = 0)$

Last time: polynomial functions and polynomial expressions. (Different expressions many define the same function,
e.g. in $\mathbb{Z}_3[x]$, $x+1$ and x^3+1 define the same function even though they are distinct expressions.)
$R[x]$ is the ring of polynomial expressions.

Today:

8.3. **The Degree of a Polynomial.**

Definition 35. *Suppose $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. If $f \neq 0$, then $deg(f)$ means the largest i such that $a_i \neq 0$. By convention, $deg(0) = -\infty$*

Example 40.

$$f = 3x - 4x^3 + 25x^4 - x^7 + 0x$$

$deg(f) = 7$

Definition 36. ***Constant Polynomial***
A constant polynomial is a polynomial of degree ≤ 0

Theorem 22. ***degree bounds on sum and product**:*

$$deg(f+g) \leq max(deg(f), def(g))$$
$$deg(fg) \leq deg(f) + deg(g)$$

(example)

Example 41. *In $\mathbb{Z}_6[x]$*

$$f = 1 + 2x$$
$$g = 1 + 3x^2$$
$$fg = 1 + 2x + 3x^2$$

$deg(fg) = 2$

Sketch of proof:

$$f = a_0 + a_1 + \cdots + a_nx^n$$
$$g = b_0 + b_1 + \cdots + b_nx^n$$

(May have zero pudded, but can assume that one of them has degree n)
$max(deg(f), deg(g)) = n$

$$f + g = (a_0 + b_0) + \cdots + (a_n + b_n)x^n$$

$deg(f+g) \leq 0$

$$fg = a_0b_0 + \cdots + (a_nb_m)x^{n+m}$$

(Here f, g, have no zero-pudding)
(What if, say $f = 0$? $fg = 0, deg(fg) = -\infty$; $deg(f) = -\infty, deg(g) = m, deg(f) + deg(g) = -\infty + m$.)

Better version for nice coefficient rings:
If D is an integral domain, then for any $f, g \in D[x], deg(fg) = deg(f) + deg(g)$

If either f or g is zero, then $deg(fg) = -\infty$ and $deg(f) + deg(g) = -\infty$

$$fg = a_0b_0 + \cdots + a_{deg}b_{deg}x^{degf+degg}$$

Corollary 4. *If D is an integral domain, then so is $D[x]$.*

Proof. $D[x]$ is commutative, unital (unity is $1 + 0x + \cdots$, not the zero ring. Suppose $f \neq 0, g \neq 0$,
Then $deg(f) \geq 0$
$deg(g) \geq 0$
$deg(fg) = deg(f) + deg(g) \geq 0$ so $fg \neq 0$ □

Warning: If R is not a domain then neither is $R[x]$.
ex: in $\mathbb{Z}_6[x]$, $(2x)(3x^5) = 0x^6$.

$$\{a_n\}_{n=1}^{\infty}, a_n = \frac{1}{n-1}$$

8.4. **Polynomial Long Division.** Calculus problem:

$$\int \frac{2x^3 + 5x - 1}{3x + 2} dx$$

Preparation:

$$(2x^3 + 5x - 1/(3x + 2) = \frac{2}{3}x^2 - \frac{4}{9}x + \frac{53}{27}... - \frac{133}{27}$$

$$\frac{2x^3 + 5x - 1}{3x + 2} = \frac{2}{3}x^2 - \frac{4}{9}x + \frac{53}{27} - \frac{133/27}{3x + 2}$$

$$\frac{f}{g} = q + \frac{r}{g}$$

$$f = gq + r \text{ (here r is 133/27)}$$

$$(deg(r) < deg(g)) \text{ (terminate condition of the algorithm}$$

8.5. **Abstract Version (Theorem on Polynomial long division):** Suppose D is an integral domainm and that $f, g \in D[x]$, such that

(1) $g \neq 0$
(2) The leading coefficient of g is a unit of D.

Then $\exists! q, r \in D[x]$ such that

(1) f = gq + r
(2) deg r < deg g

Proof. (Uniqueness)
Suppose q_1, r_1 and q_2, r_2 both satisfy condition (1) and (2)

$$f = gq_1 + r_1$$

$$f = gq_2 + r_2$$

$$gq_1 + r_1 = gq_2 + r_2$$

Now, $deg(r_2 - r_1) < deg(g)$. So, $deg(g(q_1 - q_2)) < deg(g)$.
$deg(fg) = deg(f) + deg(g)$ for integral domain. ($deg(fg) \leq (deg(f) + deg(g))$ if not)

$$deg(g) + deg(q_1 - q_2) < deg(g)$$

$$deg(q_1 - q_2) < 0$$

Therefore, $q_1 - q_2 = 0$
$q_1 == q_2$
Also, $g \cdot 0 = r_2 - r_1$, so, $r_1 = r_2$

(Existence)
Proof by Algorithm.
Given f, g, set $q_1 = 0, r_1 = f$
Let LT, LC, denote "leading term" and "leading coefficient" respectively. Definitely

$$gq_1 + r_1 = g(0) + f = f$$

(r_1 is the original f)
If $deg(r_1) deg(g)$, then terminate the algorithm. Otherwise, $\frac{LT(r_1)}{LT(g)}$ is a polynomial in $D[x]$.
Now set $q_2 = q_1 + \frac{LT(r_1)}{LT(g)}$ and set $r_2 = r_1 - g\frac{LT(r_1)}{LT(g)}$. Note:
$gq_2 + r_2 = g(q_1 + \frac{LT(r_1)}{LT(g)}) + r_1 - g\frac{LT(r_1)}{LT(g)}$

$$= gq_1 + r_1 = f$$

Also, $deg(r_2) < deg(r_1)$ Nex, if $deg(r_2) < deg(g)$, we are done. Otherwise, repeat. Eventually, we will achieve $deg(r) < deg(g)$, then we stop.

□

Last Time: Polynomial Long Division
In $D[x]$ if $f, g \in D[x]$ with $g \neq 0$ and $LC(g)$ is a unit of D, $\exists! q, r \in D[x]$ with

(1) $f = gq + r$
(2) $deg(r) < deg(g)$

8.6. **Divisibility test for Polynomials.**

Example 42.

$$(x+2)|(x^2 - x - 6)$$

$$(x^2 - x - 6) \not| (x+2)$$

$def(f) = def(g) + deg(q)$ so $def(f) \geq deg(g)$ unless $f = 0$

Let F be a field. Then $F[x]$ is an integral domain. ($F[x]$ is never a field because x has no inverse: x^{-1} is not a polynomial)

In $F[x]$, we say that $g|f$ (g divides f, or f is a multiple of g) if $\exists q \in F[x]$ with $f = gq$.

Theorem 23. *(Divisibility test for polynomials)*
$f, g \in F[x], g \neq 0$. Let q, r be as in long division. Then ($g|f \iff r = 0$)

Proof. Suppose $g|f$. Then by definition, $f = gq$ for some $q \in F[x], = gq + 0$
This shows that q is actually the quotient coming from division algorithm, and $r = 0$
OTOH, suppose $r = 0$. Then $f = gq + r = gq$, so $g|f$.

□

Example 43.

$$(2x+1)|(x^2 + 3x + 4)$$

Example 44.

$$(2x+1)|(x^2 + 3x)$$

Notation: Given $f, g \in F[x], g \neq 0$, define $f\%g$ to be the remainder when f, is divided by g.
So: $g|f \iff f\%g = 0$

8.7. **Ideals of $F[x]$.** Recall: An ideal in a ring is a subring that absorbs products.

$$Ra = \{ra | r \in R\}$$

is the principal ideal generated by a.
Note $F[x]f$ is pretty awkward notation, so we will now call this object $\langle \mathbf{f} \rangle$ (set of all polynomial multiples of f).

Example 45. *in* $\mathbb{R}[x], \langle x+1 \rangle = \{x+1, 2x+2, \pi x = \pi, x^2 - 1, \cdots\}$

Theorem 24. *Every ideal of $F[x]$ is principal, ie. of the form $\langle f \rangle$ for some fixed f.*

Proof. Let $I \subseteq F[x]$ be any ideal. I is a set (bucket) pf polynomials. $\square$

$-\infty$	*deg 0*	*deg 1*	*deg 2*	*deg 3*	$\cdots$

8.8. **Probelms.**

Problem 81. *Section 23, problems 1.*

$$f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2, g(x) = x^2 + 2x - 3, \in \mathbb{Z}_7[x].$$
$$q = (x^4 + x^3 + x^2 + x + 5)$$
$$r = 4x + 3$$

Problem 82. *Section 23, problems 2.*

$$f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2, g(x) = 3x^2 + 2x - 3, \in \mathbb{Z}_7[x].$$
$$q = 5x^4 + 5x^2 - x$$
$$r = x + 2$$

Problem 83. *Section 23, problems 3.*

$$f(x) = x^5 - 2x^4 + 3x - 5, g(x) = 2x + 1, \in \mathbb{Z}_{11}[x].$$
$$q = 6x^4 + 7x^3 + 2x^2 - x + 2$$
$$r = 4$$

Problem 84. *Section 23, problems 4.*

Problem 85. *Working in $\mathbb{Q}[x]$, find the remainder when $f(x) = x^2 + x - 3$ is divided by $x - 5$. Then compute $f(5)$.*

$$x^2 + x - 3 = (x - 5)(x + 6) + 27$$
$$f(5) = 27$$

Problem 86. *Working in $\mathbb{Z}_7[x]$, find the remainder when $f(x) = x^3 + 4x + 1$ is divided by $x - 2$. Then compute $f(2)$.*

$$x^3 + 4x + 1 = (x - 2)(x^2 + 2x + 1) + 3$$
$$f(2) = 3$$

Problem 87. *Using the theorem on polynomial long division, prove the conjecture suggested by the last two exercises.*

$$f = gq + r$$

let $x = k$, such that $g(x) = 0$, then $f(x) = 0 \cdot q + r = r$

Problem 88. *Prove the "Factor Theorem:" if F is any field, and $f \in F[x]$ is any polynomial with coefficients in F, then $f(a) = 0$ if and only if $x - a$ is a factor of f (i.e. f is a multiple of $x - a$).*

Proof. if $(x-a)$ is a factor, then $f(x) = (x-a)q, f(a) = (a-a)q = 0$.

Assume $f(a) = 0, (x-a)$ is not a factor. Then $f(x) = (x-a)q+r, r \neq 0$. Then $f(a) = 0 = (a-a)q + r = 0 + r = r, r = 0$, contradicts $r \neq 0$. Proved by contradiction.

□

Problem 89. *A "root" of a polynomial $f \in F[x]$ is an element $a \in F$ such that $f(a) = 0$. Prove that a polynomial of degree n has at most n roots. "(Hint: begin by assuming that the roots of f are $a_1, \ldots, a_r$ and then prove that $\deg(f) \geq r$.)"*

According to the previous problem, $f(a) = 0$ if and only if $(x-a)$ is a factor of f. Now assume f has degree k and has $k+1$ solutions. Then $f(x) = (x-a_1)(x-a_2)(x-a_3)\cdots(x-a_{k+1})$, multiply all $k+1$ terms, the term in the solution with the highest degree will be x^{k+1}, f has degree $k+1$.

9. **Week9**

9.1. **Definitions.** .

► **Standard representative (of an element of $\mathbf{F}[\mathbf{x}]/\langle\mathbf{m}\rangle$)**; i.e. the representative whose uniqueness is guaranteed by the theorem concerning unique representation below): Standard representative of $f+\langle m\rangle$ is the unique g with $f+\langle m\rangle = g+\langle m\rangle$ and $deg(g) < deg(m)$, turns to be $f\%m$..

► **Standard generator (of $\mathbf{F}[\mathbf{x}]/\langle\mathbf{m}\rangle$)**; usually this is denoted by α): $\alpha = x+\langle m\rangle$

9.2. **Theorems.** .

★ **Theorem concerning unique representation of elements of $\mathbf{F}[\mathbf{x}]/\langle\mathbf{m}\rangle$**:Standard representative of $f+\langle m\rangle$ is the unique g with $f+\langle m\rangle = g+\langle m\rangle$ and $deg(g) < deg(m)$, turns to be $f\%m$, g is unique.

★ **Theorem concerning $\mathbf{m}(\alpha)$ (where α is the standard generator of $F[x]/\langle m\rangle$)**: $m(\alpha) = 0$.

9.3. **Describe the Following Procedures.** .

⋆ **Procedure to calculate the standard representation of the product $(\mathbf{f}+\langle\mathbf{m}\rangle)(\mathbf{g}+\langle\mathbf{m}\rangle)$** (i.e. the "machine implementation" of multiplication in $F[x]/\langle m\rangle$): $(f+\langle m\rangle)(g+\langle m\rangle) = ((fg)\%m)+\langle m\rangle$

⋆ **Procedure to rewrite "high" powers of the standard generator α in terms of lower powers, using the theorem concerning $\mathbf{m}(\alpha)$** (i.e. the "human implementation" of multiplication in $F[x]/\langle m\rangle$)):

$$m = a_0 + a_1x + \cdots + a_{d-1}x^{d-1} + a_dx^d$$
$$a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} + a_d\alpha^d = 0$$
$$\alpha^d = -a_d^{-1}[a_0 + a_1\alpha + a_{d-1}\alpha^{d-1}]$$

Last time: Every ideal of $F[x]$ is principal, ie, generated by one element.
$I \subseteq F[x]$ is a "bucket" of polynomials.

(All)					
$-\infty$	0	1	2	3	$\cdots$

If 3, then anything after 3.

Proof. Let $I \subseteq F[x]$ be any ideal, if $I = \{0\}$ then $I = \langle 0 \rangle$. Otherwise, let d be the least non-negative integer such that I contains elements of degree d, choose any $g \in I$ with $deg(g) = d$.

We will prove that $I = \langle g \rangle$ (the set of multiples of g.

First, $\langle g \rangle \subseteq I$, because any multiple of g has the form hg and $g \in I$ and I absorbds products, So $hg \in I$.
On the other hand, choose any $f \in I$

Put $r = f\%g$. Also let q be the quotient. Then

$$f = gq + r$$

and $deg(r) < deg(g)$

$$r = f - gq$$

$f \in I, g \in I (gq \in I$, herefore, $r \in I$.
This forces $deg(r) = -\infty$, so $r = 0$, so f is a multiple of g, so $f \in \langle g \rangle$.
Every ideal is a principle. □

9.4. **Quotients of F[x].** .

Example 46.

$$\mathbb{R}[x]/\left\langle x^2 + 1 \right\rangle$$

Elements are cosets of the form $f + \langle x^2 + 1 \rangle$ (f is a polynomial).

Equality test:

$$f + \left\langle x^2 + 1 \right\rangle = g + \left\langle x^2 + 1 \right\rangle$$

iff

$$f - f \in \left\langle x^2 + 1 \right\rangle$$

iff $g - f$ is a multiple of $x^2 + 1$
iff

$$(g - f)\%(x^2 + 1) = 0$$

Example 47. *Example of quality test*

$$3x^2 + \left\langle x^2+1\right\rangle ? = 7x + \left\langle x^2+1\right\rangle$$
$$(3x^2 - 7x)\%(x^2+1) = -7x + 3 \neq 0$$

Example 48. *Example of quality test*

$$x^2 + \left\langle x^2+1\right\rangle ? = -1 + \left\langle x^2+1\right\rangle$$
$$(x^2+1)\%(x^2+1) = 0$$

Notation:

$$\alpha = x + \left\langle x^2+1\right\rangle$$

$$\begin{aligned}\alpha^2 &= (x + \left\langle x^2+1\right\rangle)(x + \left\langle x^2+1\right\rangle) \\ &= x^2 + \left\langle x^2+1\right\rangle \\ &= -1 + \left\langle x^2+1\right\rangle\end{aligned}$$

$$1_{\mathbb{R}[x]/\langle x^2+1\rangle} = 1 + \left\langle x^2+1\right\rangle$$
$$-1_{\mathbb{R}[x]/\langle x^2+1\rangle} = -1 + \left\langle x^2+1\right\rangle$$

Punch line:

$$\alpha^2 = -1 (\in \mathbb{R}[x]/\left\langle x^2+1\right\rangle)$$

Definition 37.

$$\mathbb{R}[x]/\left\langle x^2+1\right\rangle = \mathbb{C}$$

and

$$x + \left\langle x^2+1\right\rangle = i$$

More calculations in $\mathbb{C}$:

$$3x^2 + 5 + \left\langle x^2+1\right\rangle$$

Simplified:

$$(3x^2+5)/(x^2+1) = 3, r = 2$$
$$(3x^2+5) + \left\langle x^2+1\right\rangle = 2 + \left\langle x^2+1\right\rangle (r = 0)$$

In general, suppose F is a field and $m \neq 0$ is a non-zero element of $F[x]$, and form the quotient ring $F[x]/\langle m\rangle$. Any element of this ring has the form $f + \langle m\rangle$.

Claim:

$$f + \langle m\rangle = (f\%m) + \langle m\rangle$$

Proof.

$$f = mq + (f\%m)$$
$$f - (f\%m) = mq \in \langle m \rangle$$

(Difference of them lies inside the ideal, passes the equality test. □

9.5. **General Picture of F[x]/ ⟨m⟩.**

(1) Each element of this ring can be expressed in one and only one way in the form

$$f + \langle m \rangle$$

with $deg(f) < deg(m)$.

Proof. Any element of $F[x]/\langle m \rangle$ has the form $f + \langle m \rangle$. But

$$f + \langle m \rangle = (f\%m) + \langle m \rangle$$

($f\%m$ has degree $< deg(m)$).

Uniqueness: Suppose $f_1 + \langle m \rangle = f_2 + \langle m \rangle$ with $deg(f_1) < deg(m)$ and $deg(f_2) < deg(m)$.

$$f_1 - f_2 \in \langle m \rangle$$
$$f_1 - f_2 = mq$$
$$f_1 - f_2 + mq$$

if $q \neq 0$, $deg(mq) \geq deg(m)$. Then we have a contradiction because $deg(f_2)$ is too low to cancel $LT(mq)$, forcing $deg(f_2) \geq deg(m)$. So $q = 0$ and $f_1 - f_2 = 0$, $f_1 = f_2$.

□

(2) Addition:

$$(f_1 + \langle m \rangle) + (f_2 \langle m \rangle) = (f_1 = f_2) + \langle m \rangle$$

(3) Multiplication:

$$(f_1 + \langle m \rangle)(f_2 + \langle m \rangle) = f_1 f_2 + \langle m \rangle$$
$$= ((f_1 f_2)\%m) + \langle m \rangle$$

$\mathbb{C} = \mathbb{R}[x]/\langle x^2 + 1 \rangle$

Each element is written uniquely in the formm $f + \langle x^2 + 1 \rangle$, $deg(f) < 2$.

$$f + \left\langle x^2 + 1 \right\rangle = (a + bx + \left\langle x^2 + 1 \right\rangle, a, b \in \mathbb{R}$$
$$a + bi = (a + \left\langle x^2 + 1 \right\rangle) + (b + \left\langle x^2 + 1 \right\rangle)(x + \left\langle x^2 + 1 \right\rangle)$$
$$= (a + bx) + \left\langle x^2 + 1 \right\rangle$$

each element of $\mathbb{C}$ is uniquely of the form $a + bi (a, b \in \mathbb{R})$

Last time: The ring $F[x]/\langle m\rangle$. Ex: $\mathbb{R}[x]/\langle x^2+1\rangle = \mathbb{C}$

Example 49. $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ *($\mathbb{Z}_2$ is a field)*

$$F[x]/\langle m\rangle = \{f+\langle m\rangle \,|deg(f) < deg(m)\}$$

$$\mathbb{Z}_2[x]/\left\langle x^2+x+1\right\rangle = \{f+\left\langle x^2++x1\right\rangle \,|deg(f) < 2 \leq 1\}$$

$$a+bx+\left\langle x^2+x+1\right\rangle \,|a,b\in\mathbb{Z}_2\}$$

$$\{0+\left\langle x^2+x+1\right\rangle, 1+\left\langle x^2+x+1\right\rangle, x+\left\langle x^2+x+1\right\rangle, x+1+\left\langle x^2+x+1\right\rangle\}$$

$$\begin{aligned} 0+\left\langle x^2+x+1\right\rangle &\equiv 0\\ 1+\left\langle x^2+x+1\right\rangle &\equiv 1\\ x+\left\langle x^2+x+1\right\rangle &\equiv \alpha\\ 1+x+\left\langle x^2+x+1\right\rangle &= 1+\alpha\\ \mathbb{Z}_2[x]/\left\langle x^2+x+1\right\rangle &= \{0,1,\alpha,1+\alpha\} \end{aligned}$$

$+$	*0*	*1*	α	$1+\alpha$
0	*0*	*1*	α	*1+* α
1	*1*	*0*	*1+* α	α
α	α	*1+* α	*0*	*1*
1 + α	*1+* α	α	*1*	*0*

$\cdot$	*0*	*1*	α	$1+\alpha$
0	*0*	*0*	*0*	*0*
1	*0*	*1*	α	*1+* α
α	*0*	α	*1* + α	*1*
1 + α	*0*	*1* + α	*1*	α

$$\alpha^2 = (x+\left\langle x^2+x+1\right\rangle)(x+\left\langle x^2+x+1\right\rangle) = x^2+\left\langle x^2+x+1\right\rangle = (1+x)+\left\langle x^2+x+1\right\rangle$$

$$(x^2)/(x^2+x+1), r = 1+x$$

Units of $\mathbb{Z}_2/\langle x^2+x+1\rangle$*:* $\{1,\alpha,1+\alpha\}$
This is a field. Everything except from 0 *is a unit. This field has a name. It's called* $GF(4)$*, Galois field.*

Initial Morphism into GF(4) (From $\mathbb{Z}$ to $GF(4)$)

x	$\iota(x)$
0	0
1	1
2	0
3	1
4	0
$\cdots$	$\cdots$

$\mathbb{Z} \to GF(4)$; $Char(GF(4)) = 2$

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Prime Subring:

$+$	0	1
0	0	1
1	1	0

$+$	0	1
0	0	0
1	0	1

For Programmer:

$$GF(4) = \{a + bx | a, b \in \mathbb{Z}_2\}$$

(Can use 2 bits to store)

Example 50.

$$\mathbb{Z}_2[x]/\left\langle x^3 + x^2 + 1 \right\rangle = R$$
$$R = \{f + \left\langle x^3 + x^2 + 1 \right\rangle | deg(f) < 3 (\leq 2)\}$$
$$= \{a + bx + cx^2 + \left\langle x^3 + x^2 + 1 \right\rangle | a, b, c \in \mathbb{Z}_2$$
$$|R| = 8$$
$$R = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

(make the table here)

It turns out that this is also a field, called $GF(8)$.

Example 51.

$$\mathbb{Z}_3[x]/\left\langle x^2 + 1 \right\rangle$$

is also a field, called $GF(9)$.

If $\mathbb{Z}_p[x]/\langle m\rangle$ is a field, it's called $GF(p^{deg(m)})$
Today

9.6. **Basic rule of arithmetic and the human interface to $\mathbf{F[x]/\langle m\rangle}$".**
.

$$GF(4) = \mathbb{Z}_2[x]/\left\langle x^2+x+1\right\rangle$$
$$\alpha = x + \left\langle x^2+x+1\right\rangle$$
$$m(\alpha) = \alpha^2+\alpha+1$$
$$= (x+\langle m\rangle)(x+\langle m\rangle)+(x+\langle m\rangle)+(1+\langle m\rangle)$$
$$= x^2+x+1+\langle m\rangle$$
$$m+\langle m\rangle$$
$$= 0+\langle m\rangle$$

Thus: $\alpha^2+\alpha+1=0, m(\alpha)=0$. This is fundamental rule of arithmetic in $GF(4)$.

$$\alpha^2+\alpha+1=0$$
$$\alpha^2 = -\alpha-1$$
$$= \alpha+1(\in \mathbb{Z}_2)$$

	0	1	α	$1+\alpha$
0				
1				
α				
$\alpha+1$				

Example 52.

$$\mathbb{C} = \mathbb{R}[x]/\left\langle x^2+1\right\rangle$$
$$\alpha = x+\langle m\rangle$$
$$m(\alpha) = \alpha^2+1=0$$
$$\alpha^2 = -1$$

Example 53.

$$\mathbb{Q}[x]/\left\langle x^2-2\right\rangle$$

(Hippasus): There is no element of $\mathbb{Q}$ *whose square is 2.*

$$\alpha = x+\langle m\rangle$$
$$m(\alpha) = \alpha^2-2=0$$
$$\alpha^2 = 2$$

In general, if we want to "solve" the equation $m(x) = 0$, we can always do this by forming the ring $R = F[x]/\langle m \rangle$. Then $\alpha = x + \langle m \rangle$ is a solution of $m(x) = 0$. (Fundamental rule of arithmetic is something we use to proof there is always a solution with α).
Kronecker: "The equation is its own solution."
WARNING: The R we just constructed may turn to be a really bad ring.

Example 54.

$$R = \mathbb{R}[x]/\left\langle x^2 - 1 \right\rangle$$
$$R = \{a\alpha + b | a, b \in \mathbb{R}\}$$
$$(\alpha - 1)(\alpha + 1) = \alpha^2 - 1 = 0$$

But

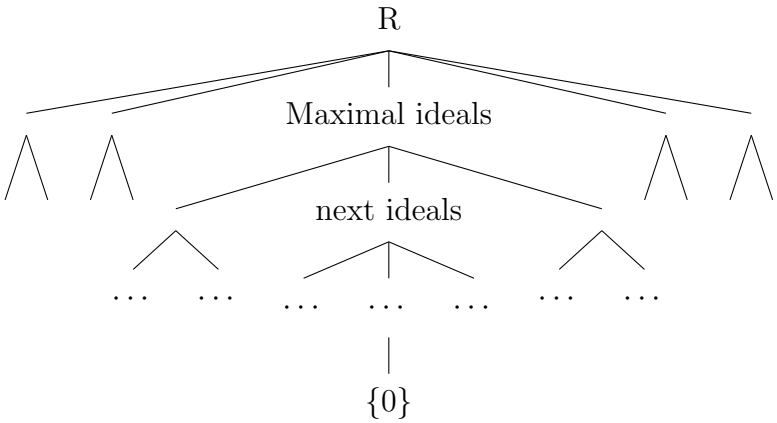
$$\alpha - 1 \neq 0$$
$$\alpha - 1 = x - 1 + \left\langle x^2 - 1 \right\rangle$$
$$0 = 0 + \left\langle x^2 - 1 \right\rangle$$
$$\alpha - 1 = 0 \iff x - 1 - 0 \in \left\langle x^2 - 1 \right\rangle$$

$\iff$ *$x - 1$ is a multiple of $x^2 - 1$.*

$$\alpha + 1 \neq 0$$

R is not even an integral domain.

NOTE:
$\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is a field.
$\mathbb{R}[x]/\langle x^2 - 1 \rangle$ is not a domain.
$\mathbb{Z}/3\mathbb{Z}$ is a field.
$\mathbb{Z}/4\mathbb{Z}$ is not a domain.



9.7. **Problems.** .

Problem 90. *Let R denote the quotient ring $\mathbb{Z}_2[x]/\langle x^2+1\rangle$. List the elements of R, then make a multiplication table. Is R a field?*

$$F[x]/\langle m\rangle = \{f + \langle m\rangle \,|deg(f) < deg(m)\}$$
$$\mathbb{Z}_2[x]/\left\langle x^2+1\right\rangle = \{f + \left\langle x^2+1\right\rangle \,|deg(f) < 2 \leq 1\}$$
$$= \{a + bx + \left\langle x^2+x+1\right\rangle \,|a, b \in \mathbb{Z}_2\}$$
$$\{0 + \left\langle x^2+1\right\rangle, 1 + \left\langle x^2+1\right\rangle, x + \left\langle x^2+1\right\rangle, x+1 + \left\langle x^2+1\right\rangle\}$$
$$0 + \left\langle x^2+1\right\rangle \equiv 0$$
$$1 + \left\langle x^2+1\right\rangle \equiv 1$$
$$x + \left\langle x^2+1\right\rangle \equiv \alpha$$
$$1 + x + \left\langle x^2+1\right\rangle = 1 + \alpha$$
$$\mathbb{Z}_2[x]/\left\langle x^2+1\right\rangle = \{0, 1, \alpha, 1+\alpha\}$$

$\cdot$	*0*	*1*	α	$1+\alpha$
0	*0*	*0*	*0*	*0*
1	*0*	*1*	α	*1+* α
α	*0*	α	*1*	$1+\alpha$
1 + α	*0*	*1* + α	$1+\alpha$	0

$$\alpha^2 = (x + \left\langle x^2+1\right\rangle)(x + \left\langle x^2+1\right\rangle) = x^2 + \left\langle x^2+1\right\rangle = 1 + \left\langle x^2+1\right\rangle$$
$$x^2/(x^2+1), r = 1$$

Not a field, not all non-zero elements are units.

Problem 91. *Let $GF(8)$ denote the quotient ring $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$. List the elements of $GF(8)$. Be sure to list each element only once. (You will probably find it more pleasant to write them in terms of the standard generator α rather than using coset notation.)*

$$\{0, 1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, 1+\alpha+\alpha^2, \alpha+\alpha^2\}$$

Problem 92. *Working in $GF(8)$, compute the sum $(1+\alpha^2)+(1+\alpha)$.*

$$(1+\alpha^2)+(1+\alpha) = 2+\alpha+\alpha^2 = \alpha+\alpha^2$$

Problem 93. *Using the "machine implementation" of multiplication in $GF(8)$, compute the product $(1+\alpha^2)(1+\alpha)$. Be sure to write your answer in its standard representation.*

$$(1+\alpha^2)(1+\alpha) = 1+\alpha^2+\alpha+\alpha^3$$

$$\alpha^3/(\alpha^3+\alpha+1), r = \alpha+1$$
$$1+\alpha^2+\alpha+\alpha^3 = 1+\alpha^2+\alpha+\alpha+1 = \alpha^2$$

Problem 94. *Working in $GF(8)$, find a formula for α^3 in terms of lower powers of α. "(Hint: use the theorem regarding $m(\alpha)$.)"*

$$m(\alpha) = \alpha^3+\alpha+1 = 0$$
$$\alpha^3 = -\alpha-1 = \alpha+1$$

Problem 95. *Use the formula you found above to compute the standard representations of α^4, α^5, α^6, and α^7.*

$$\alpha^4 = \alpha\cdot\alpha^3 = \alpha^2+\alpha$$
$$\alpha^5 = \alpha\cdot\alpha^4 = \alpha^3+\alpha^2 = 1+\alpha+\alpha^2$$
$$\alpha^6 = \alpha\cdot\alpha^5 = \alpha+\alpha^2+\alpha^3 = \alpha+\alpha^2+\alpha+1 = \alpha^2+1$$
$$\alpha^7 = \alpha^6\cdot\alpha = \alpha^3+\alpha = \alpha+1+\alpha = 1$$

Problem 96. *Redo your calculation of $(1+\alpha^2)(1+\alpha)$, this time avoiding the "machine implementation" in favor of the formula you found above for α^3. Verify that you obtain the same answer.*

$$(1+\alpha^2)(1+\alpha) = 1+\alpha^2+\alpha+\alpha^3 = 1+\alpha^2+\alpha+1+\alpha = \alpha^2$$

Problem 97. *Suppose $m \in \mathbb{Z}_p[x]$ is a polynomial of degree d. Compute the cardinality of the ring $\mathbb{Z}_p[x]/\langle m\rangle$. "(Hint: use the theorem on unique representation of elements. How many choices are there for each coefficient, and how many coefficients are there?)"*

$$p^d$$

Problem 98. *Verify that the formula you found above correctly predicts the number of elements of $GF(8)$.*

$$2^3 = 8$$

10. **Week10**

10.1. **Definitions.** .

▶ **Maximal ideal**: I is maximal if

(1) $I \neq R$
(2) $I \subseteq J \subseteq J \subseteq R \Rightarrow J = I || J = R$.

▶ **Divisibility relation (in a domain D; i.e. a|b if and only if...)**: let D be an integral domain, $a|b$ if $\exists c \in D$ with $b = ac$.

▶**Associate relation (in a domain D; i.e. $\mathbf{a \sim b}$ if and only if...)**: In D, $a \sim b$ iff $a|b$ and $b|a$. (a is an associate of b.)

▶ **Associate class (of an element of a domain D)**: The equivalence class $[a]_\sim$ is called the associate class of a.

$$[a]_\sim = \{b | a \sim b\}$$

10.2. **Theorems.** .

★ **Theorem characterizing the ideals I for which R/I is a field**: R/I is a field iff I is maximal.

★ **Containment criterion for principal ideals (i.e. $\langle \mathbf{a} \rangle \subseteq \langle \mathbf{b} \rangle$ if and only if...)**: In D. $\langle b \rangle \subseteq \langle a \rangle$ iff $a|b$.

★ **Equality criterion for principal ideals (i.e. $\langle \mathbf{a} \rangle = \langle \mathbf{b} \rangle$ if and only if...)**: $a \sim b$

★ **Properties of the associate relation (i.e. $\sim$ is an...)**: $\sim$ is an equivalence relation on D:

★ **Characterization of the associate class $[\mathbf{a}]_\sim$**: The equivalence class $[a]_\sim$ is called the associate class of a. $[a]_\sim = \{ua | u \in U(D)\}$ (u is unit)

★ **List of units in $\mathbb{Z}$**: $\{1, -1\}$.

Last time: $F[x]/\langle m\rangle$

$$\alpha = x + \langle m\rangle$$
$$F[x]/\langle m\rangle = \{a_0, a_1\alpha + a_2\alpha^2 + \cdots + a_{deg(m)-1}\alpha^{deg(m)-1} | a_i \in F\}$$
$$m(\alpha) = 0$$

But this may turn out to be a bad ring.

This time: when will $F[x]/\langle m\rangle$ be a field? More generally, when is R/I a field?.
Result: I is a maximal ideal.Standing notation:
R is a commutative, unital ring.
$I \in R$ is an ideal of R.

Definition 38. ***Maximal Ideal***
I is maximal if

(1) $I \neq R$
(2) $I \subseteq J \subseteq J \subseteq R \Rightarrow J = I || J = R.$

Theorem 25. *R/I is a field iff I is maximal.*

Proof. First suppose that I is maximal.
R/I is commutative and unital because R is.
R/I is not a zero ring because $I \neq R$
Suppose $a + I \neq 0 + I$, then $a - 0 \notin I$, so $a \notin I$.
Let

$$J = \{ra + i | r \in R, i \in I\}$$

Claim: J is an ideal.

- $0 \in J$ because $0 = 0a(\in R) + 0(\in I)$.
- Suppose $j_1, j_2 \in J$, write $j_1 = r_1a + i_1, j_2 = r_2a + i_2$. $j_1 + j_2 = (r_1 + r_2)a + (i_1 + i_2) \in J$.
- Suppose $j \in J$ and $s \in R$. Write $j = ra+i$, $sj = (sr)a+si \in J$. $sr \in R, si \in I$.

Claim 2: $I \subseteq J$. Choose $i \in I$. Write $i = 0a + i \in J$.
Claim 3: $a \in J$, because $a = 1a + 0$.
Thus, J is an ideal with $I \subseteq J \subseteq R$, but $I \neq J$. Maximality implies$J = R$.
In particular, $I \in J$, choose r, i with $ra + i = 1$ (particular r, i)
Then, $(r + I)(a + I) = ra + I = 1 + I$ (because $ra - 1 = -i \in I$)
So $a + I$ has inverse $r + I$.

Conversely, suppose that R/I is a field. Then R/I is not a zero ring. So $I \neq R$. Now suppose $I \subseteq J \subseteq R$

Case1:

(Hypothesis, $I \in J$)

□

Friday

$$F[x]/\langle m\rangle$$

can be implemented on computers.
Useful for:

- mystical approach to equation-solvings. $(m(x) = 0)$
- Symbolic computation (Same thing as the first one)

But $F[x]/\rangle m\rangle$ may be a bad ring.
Question: when will $F[x]/\langle m\rangle$ be a field?
On Monday: R/I is a field $\iff$ I is a maximal ideal.
Next: Ideal diagram of $F[x]$.

(Need a Graph here)

This must have something to do with factorizations of polynomials.

10.3. **Factorization Theory.** .
let D be an integral domain.
(Examples: $D = \mathbb{Z}||D = F[x]$).

Definition 39. *$a|b$ if $\exists c \in D$ with $b = ac$.*

Theorem 26. *In D. $\langle b\rangle \subseteq \langle a\rangle$ iff $a|b$.*

Proof. Suppose thT $\langle b\rangle \in \langle a\rangle, b = 1 \cdot b$, so $b \in \langle b\rangle$, sp $b \in \langle a\rangle$, so $a|b$.

OTOH suppose $a|b$. Then $b \in \langle a\rangle$. Thus, $\langle a\rangle$ is an ideal that contains b. But $\langle b\rangle$ is the smallest ideal that contains b. Thus $\langle b\rangle \subseteq \langle a\rangle$. □

Example 55.

$$\langle 25\rangle \in \langle 5\rangle$$

$$5|25$$

Example 56.

$$\left\langle x^2 - 1\right\rangle \subseteq \langle x + 1\rangle$$

Example 57. *In* $\mathbb{R}[x]$,

$$\langle 2x+2\rangle \subseteq \langle x+1\rangle$$

Example 58. *In* $\mathbb{R}[x]$,

$$\langle x+1\rangle \subseteq \langle 2x+2\rangle$$

$$x+1=\frac{1}{2}(2x+2)$$

In conclusion: in $\mathbb{R}[x]$, $x+1=2x+2$.

Definition 40. *in* D, $a\sim b$ *iff* $a|b$ *and* $b|a$. *(*a *is an associate of* b.*)*

Theorem 27. $\sim$ *is an equivalence relation on* D.

Proof. $a\sim b$ iff $a|b$ and $b|a$.
iff $\langle b\rangle \subseteq \langle a\rangle$ and $\langle a\rangle \subseteq \langle b\rangle$
iff $\langle b\rangle = \langle a\rangle$.
(= is an equivalence relation.) □

The equivalence class $[a]_\sim$ is called the associate class of a.

Example 59. *Examples in* $\mathbb{Z}$*:*

$$[2]_\sim = \{2,-2\}$$

$$[6]_\sim = \{6,-6\}$$

$$[0]_\sim - = \{0\}$$

Example 60. *Examples in* $\mathbb{R}[x]$*:*

$$[x+1]_\sim = \{x+1, kx+k\}$$

Theorem 28. *The equivalence class* $[a]_\sim$ *is called the associate class of* a. $[a]_\sim = \{ua|u\in U(D)\}$ *(*u *is unit)*

Proof. Suppose $x\in\{ua|u\in U(D)\}$.
Write $x=ua$ for some fixed$u\in U(D)$.
So $a|x$. Also, $u^{-1}x=a$, so $x|a$. So $x\sim a$ and thus $x\in[a]_\sim$.
OTOH, suppose $x\in[a]_\sim$. The n $x\sim a$. Thus $x|a$ and $a|x$. So $a=bx$ for some b, and $x=ca$ for some c.
Then$a=bca$.
Case 1: $a\neq 0$. Then $1=bc$ (cancellation law in integral domain).
Thus, c is a unit with $c^{-1}=b$. Then $x=ca$, so $x\in\{ua|u\in U(D)\}$.
Case 2: $a=0$. Then $x=x(0)=0$.
So $x=1\cdot a$, and again $x\in\{ua|u\in U(D)\}$. □

10.4. **Problems.** .

Problem 99. *Suppose $u \in F[x]$ is a unit. Prove the* $\deg(u) = 0$. *"(Hint: start with the equation $u \cdot u^{-1} = 1$, and take degrees of both sides.)"*

$$u \cdot u^{-1} = 1$$
$$deg(u \cdot u^{-1}) = deg(1) = 0$$
$$deg(u \cdot u^{-1}) \leq deg(u) \cdot deg(u^{-1}) = 0$$
$$deg(u) = 0, deg(u^{-1}) \leq 0 || deg(u^{-1}) = 0, deg(u) \leq 0$$

if $deg(u) = \infty, u = 0$, if $deg(u^-1) = -\infty, u^{-1} = 0$, 0 is not a unit. Therefore, both $deg(u), deg(u^{-1}) = 0$

Problem 100. *Suppose $f \in F[x]$ has degree zero. Show that f is a unit. "(Hint: remember that F is a field. What sort of polynomials have degree zero?)"*

f has degree 0, therefore, f is a non-zero constant polynomial. f is also an element in F, F is a field, every non-zero element is a unit. f is a unit in F, its inverse $f^{-1} \in F$ is also a non-zero constant polynomial in $F[x]$. Therefore, f is a unit in $F[x]$.

Problem 101. *Let D be any integral domain. Prove that $a \in D$ is a unit if and only if $a \sim 1$.*
If $a \sim 1, a|1, 1 = ac; 1|a, a = 1 \cdot c$. $a^{-1} = c, a = c$. a has an inverse $a \in D$, a is a unit.
if $a \not\sim 1$, if $a \nmid 1, 1 \neq ac$, a doesn't have an inverse. If $1 \nmid a$, there is no identity element. It is not unital and therefoir not integral domain.

Problem 102. *Suppose $u \in D$ is a unit and $u \sim v$. Prove that v is also a unit.*

$$u \sim v$$
$$u|v, v|u$$
$$1|u, u|1$$
$$1|u, u|v : u = c_1 \cdot 1, v = c_2 u$$
$$v = c_2 \cdot c_1 \cdot 1 : 1|v$$
$$v|u, u|1 : u = c_3 v, 1 = c_4 u$$
$$1 = c_4 \cdot c_3 v : v|1$$
$$1|v \&\& v|1$$

v is also a unit.

Problem 103. *An element $a \in D$ is said to be "irreducible" if it is not zero, not a unit, and given any factorization $a = bc$, either b is a unit or c is a unit. Describe the irreducible elements of $\mathbb{Z}$.*
Let b be a unit 1, and $c = 5$.

$$a = bc = 1 \cdot 5 = 5$$

a is not zero and a doesn't have an inverse and therefore not a unit. Any $c \neq 1, -1$ would satisfy it.
Therefore, irreducible elements of $\mathbb{Z}$ are $\{p | p \text{ is a prime}\}$.

Problem 104. *Working in $F[x]$ where F is some field, show that any polynomial of degree one is irreducible. "(Hint: suppose $\deg(f) = 1$ and $f = gh$. Taking the degree of both sides of this equation gives $1 = \deg(g) + \deg(h)$. What are all the possible values for the ordered pair $(\deg(g), \deg(h))$?)"*

$$f = gh$$
$$1 = deg(g) + deg(h)$$
$$deg(g) = 1, deg(h) = 0$$

or

$$deg(g) = 0, deg(h) = 1$$

one of g and h must be constant polynomial, and another must be degree one polynomial. The constant polynomial should also be an element in F, which has a unit in F, and this unit is also in $F[x]$. Assume the degree 1 polynomial has a unit:

$$gg^{-1} = 1, hh^{-1} = 1, g^{-1}gh^{-1}h = 1 = fg^{-1}h^{-1}$$
$$deg(g) + deg(g^{-1}) + deg(h) + deg(h^{-1}) = 0$$
$$1 + 0 + deg(g^{-1}) + deg(h^{-1}) = 1$$
$$deg(g^{-1}) + deg(h^{-1}) = 0$$

g^{-1}, h^{-1} are both constant polynomial. However, (assume h is the one not constant) $deg(hh^{-1}) = deg(h) + deg(h^{-1} = 1 + 0 = 1$, $hh^{-1} \neq 1$. Inverse of degree 1 polynomial h doesn't exist.

Problem 105. *Working in $F[x]$, show that a polynomial f of degree two is irreducible if and only if it has no roots in F. "(Hint 1: you will need the Factor Theorem that you proved in "Assignment 9". Hint 2: suppose you have a factorization $f = gh$ in which neither g nor h is a unit. What are the degrees of g and h?)"*

If a polynomial f of degree 2 has a root α, then it can be written as $f = (x - \alpha)h$ (which is linear and makes f has non-trivial factoriztion),

$x - \alpha$ is degree 1, h has to be degree 1 to make f degree 2. However, from question 6, polynomial of degree 1 is not a unit. Therefore, both g and h in this case are not units, which is against the definition of irreducible.

If it has no roots, $f = gh$, g, h cannot be degree 1 polynomials. Instead, they will be a degree 0 polynomial and a degree 2 polynomial. Degreen 0 polynomial g has an inverse, it is a unit. Degree 2 polynomial h has no inverse, because $deg(hh^{-1}) = deg(h) + deg(h^{-1}), 0 = 2 + deg(h^{-1})$, but degree cannot be -2 to satisfy the equation. Therefore, h (degree 2) is not a unit.

$$0, 2$$

$$2, 0$$

Problem 106. *Working in $F[x]$, show that a polynomial f of degree three is irreducible if and only if it has no roots in F. "(Hint: this is very similar to the previous exercise.)"*
Same as the previous question, if f has a root, then it can be written as a degree 1 polynomial and a degree 2 polynomial, both have no units. If it has not, it can be written as degree 0 and degree 3.

Problem 107. *Give an example of a field F and a polynomial $f \in F[x]$ of degree four, which has no roots but is nevertheless reducible. "(Hint: this is much easier than it looks. The most familiar examples are those with $F = \mathbb{R}$. You simply need to find a pair of degree-two polynomials with no roots, and multiply them.)"*

In $\mathbb{R}[x]$, $x^4 + 5x^2 + 6$ is reducible but has no roots:

$$x^4 + 5x^2 + 6 = (x^2 + 2)(x^2 + 3)$$

Problem 108. *Does the example you produced in the last problem invalidate the reasoning you used in the previous two? If not, at exactly what point does the reasoning you used in the previous two exercises break down in the case of degree-four polynomials?*

The combination of degrees can be $2, 2$, can these two degree 2 polynomial can have no non-trivial factorization, which means that no linear term, no root. However, degree 2 and degree 2 make this degree 4 polynomial have non-trivial factorization.

Problem 109. *Working once more in a general integral domain D, prove that if a is irreducible and $a \sim b$, then b is also irreducible.*
Suppose $b = xy$, $b = ua$, $ua = xy, a = u^{-1}xy$, a is irreducible, so either

y is a unit or $(u^{-1}x)$ is a unit.

$$u^{-1}x = v$$

(v is a unit)

$$x = uv$$

11. Week11

11.1. Irreducible. .

In $\mathbb{R}[x]$:

$$x^2 - x - 6 = (x-3)(x+2) = 1 \cdot (x^2 - x - 6)$$

Definition 41. ***Trivial Factorization***
In an integral domain D:
The factorization $a = bc$ is said to be ***trivial*** *is one of b, c is a unit.*
Note: Every element has many trivial factorizartion: for any unit u, we can write

$$a = u(u^{-1}a)$$

Definition 42. *$a \in D$ is said to be irreducible if it is*

(1) *not zero*
(2) *not a unit*
(3) *has no non-trivial factorization*

Example 61. *in $\mathbb{Z}$, 7 is irreducible, but 6 is not irreducible, because $6 = 2 \cdot 3$.*

In $\mathbb{R}[x]$, $x - 4$ is irreducible.

$$x - 4 = fg$$

$$1 = deg(f) + deg(g)$$

They have to be 1 and 0. All degree 1 polynomials have to be irreducible.

Suppose $f \in F[x]$ with $deg(f) = 2$. Claim: f is irreducible $\iff$ f has no roots in F.
Suppose f has a root, $a \in F$, i.e. $f(a) = 0$. Then $(x-a)|f$, say $f = (x-a)q$.

$$a = 1 + deg(q) \Rightarrow deg(q) = 1$$

$$f = (x-a)q$$

non-trivial factorization. So, f is reducible.
★ Conversely, if f is reducible, then (suppose non trivial) $f = gh$ with $deg(g) = deg(h) = 2 = deg(g) + deg(h)$ $(deg(g) = deg(h) = 1, deg(g) + deg(h) = 2)$.

$$0, 2$$

$$2, 0$$

$$1, 1$$

So g is linear if it has non-trivial factorization, and every linear has a root: $ax + b$ has $-ba^{-1}$ as a root.
(any factorization with a $deg = 1$ factor has a root).

Example 62. *In* $\mathbb{R}[x]$, $x^2 + 1$ *is irreducible.*

Note: The same idea is valid for cubic polynomaials: $deg(f) = 3$, then f is irreducible $\iff$ f has no roots.
This will be false for higher degrees.

Example 63. *In* $\mathbb{R}[x]$, $x^4 + 5x^2 + 6$ *is reducible but has no roots:*

$$x^4 + 5x^2 + 6 = (x^2 + 2)(x^2 + 3)$$

Theorem 29. *In* $F[x]$*, the ideal* $\langle m \rangle$ *is maximal if and only if* m *is irreducible.*

Proof. First suppose m is irreducible. Suppose further that $\langle m \rangle \subseteq J \subseteq F[x]$. But J is a principle ideal, say $J = \langle f \rangle$.

$$\langle m \rangle \subseteq \langle f \rangle \subseteq \langle 1 \rangle$$

Thus $1|f$ and $f|m$.Thus $m = fg$ for some g. This must be a trivial factorization. i.e. either f or g must be a unit.
Case 1: if f is a unit, then $\langle f \rangle$ contains a unit, it must be an improper ideal. $\langle f \rangle = F[x]$.
Case 2: Suppose g is a unit. Then m is a unit multiple of f, so $m \sim f$. Associate class generate same ideals. $\langle m \rangle = \langle f \rangle$. $\langle m \rangle$ is maximal.

OTOH, Suppose m is reducible, then either

(1) $m = 0$, or
(2) m is a unit, or
(3) m has a non-trivial factorization.

Case 1: $\langle 0 \rangle$ is not maximal because

(1) $\langle 0 \rangle \subsetneq \langle x \rangle \subsetneq F[x]$.
(2) If m is a unit then $\langle m \rangle = F[x]$ is bot maximal.
(3) $m = fg$ with neither f or g a unit, $f|m$ but $f \not\sim m$. $\langle m \rangle \subsetneq \langle f \rangle \subsetneq F[x]$.
So $\langle m \rangle$ is not maximal.

□

11.2. **prime ideal.** .
R/I is a field $\iff$ I is maximal.
$F[x]/\langle m\rangle$ is a field
$\iff$ $\langle m\rangle$ is maximal,
$\iff$ m is irreducible.

Example 64. *$\mathbb{Z}/\langle n\rangle$ is a field*
$\iff$ $\langle n\rangle$ is maximal
$\iff$ n is irreducible.
(Same proof as in polynomial case.)

R/I is an integral domain $\iff$ I is a prime ideal.

Definition 43. *Let R be a commutative, unital ring, I an ideal of R. I is a prime ideal if*

(1) *$I \neq R$, and*
(2) *$ab \in I \Rightarrow$ either $a \in I$ or $b \in I$.*

Example 65. *Non-examples in $\mathbb{Z}$:*

(1) *$\langle 1\rangle$ is not prime because $\langle 1\rangle = \mathbb{Z}$*
(2) *$\langle 6\rangle$ is not prime: $2 \cdot 3 \in \langle 6\rangle$, but $2 \notin \langle 6\rangle$ and $3 \notin \langle 6\rangle$*

Example 66. *Examples from $\mathbb{Z}$: $\langle 0\rangle$ is prime:*
$\langle 0\rangle = \{0\} \neq \mathbb{Z}$
$ab \in \{0\} \Rightarrow ab = 0 \Rightarrow$ *either $a = 0$ or $b = 0$.*

R is an integral domain $\iff$ $\{0\}$ is a prime ideal.
In $\mathbb{Z}$:
$\langle 3\rangle$ is prime:
$\langle 3\rangle \neq \mathbb{Z}$, also if $ab \in \langle 3\rangle$, then $3|ab$ so $3|a$ and $3|b$.

Example 67. *Non-example in $\mathbb{R}[x]$.*
$\langle x^2 - 1\rangle$ is not prime:

$$(x+1)(x+1) \in \left\langle x^2 - 1\right\rangle$$

but

$$x - 1 \notin \left\langle x^2 - 1\right\rangle$$
$$x + 1 \notin \left\langle x^2 - 1\right\rangle$$

Theorem 30. *R/I is an integral domain $\iff$ I is prime.*

Proof. Suppose I is prime. R/I is commutative and unital because R is,
R/I is not a zero ring because $R \neq I$.

Finally, we verify the zero-product property:
Suppose

$$(a+I)(b+I) = 0+I$$
$$ab+I = 0+I$$
$$ab-0 \in I$$
$$ab \in I$$

either $a \in I$ or $b \in I$,

$$a-0 \in I$$
$$a+I = 0+I$$

Same thing for b.
$R/\langle 0\rangle \backsimeq R$ domain iff $\langle 0\rangle$ is prime.
In $F[x]$, $\langle 0\rangle$ is prime because $F[x]$ is an integral domian.

□

Theorem 31. *Every maximal ideal is prime.*

Proof. Suppose I is maximal, then R/I is a field, then R/I is an integral domain, then I is prime. □

Warning: Not every prime ideal is maximal.

Example 68. *in $\mathbb{Z}$ or in $F[x]$, $\langle 0\rangle$ is prime.*
$\langle 0\rangle \subsetneq \langle 2\rangle \subsetneq \mathbb{Z}$
$\langle 0\rangle \subsetneq \langle x\rangle \subsetneq F[x]$

Example 69. *in $\mathbb{R}[x,y]$,*
$\langle 0\rangle \subsetneq \langle x\rangle \subsetneq \langle x,y\rangle \subsetneq \mathbb{R}[x,y]$
$\subsetneq$ means contained in, not equal. ($\not\subseteq$ means not contained in).

Note: Su[ppose $m \in F[x]$ is not zero, not a unit, but has a non-trivial factorization $m - fg$. Then $\langle m\rangle$ is not prime.

$$fg \in \langle m\rangle$$

but

$$f \notin \langle m\rangle \, (deg(f) < deg(m))$$
$$g \notin \langle m\rangle$$

Structure of $F[x]/\langle m\rangle$:

- If m is a unit, $F[x]/\langle m\rangle = \{0\}$
- If $m = 0$, tehn $F[x]/\langle m\rangle \backsimeq F[x]$ is an integral domain.
- If m is irreducible, $F[x]/\langle m\rangle$ is a field.
- If m can be factored, $F[x]/\langle m\rangle$ has zero divisor.

Example 70. $\mathbb{R}[x]/\langle x^2 = 1\rangle$ *is a field.* x^2+1 *is degree* 2 *with no roots, so it is irreducible.*

Example 71. $\mathbb{R}[x]/\langle x^2-1\rangle$ *has zero divisor.*

Example 72. $\mathbb{R}[x]/\langle 3\rangle = \{0\}$
$\mathbb{R}[x]/\langle 0\rangle \backsimeq \mathbb{R}[x]$ *(isomorphic)*

Example 73. $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ *is a field.*

x	x^2+x+1
0	*1*
1	*1*

No roots. Irreducible.

Example 74. $\mathbb{Z}_2[x]/\langle x^2+1\rangle$ *has zero-divisor*

x	x^2+1
0	*1*
1	*0*

It has root and non-trivial factoriztion:

$$x^2+1=(x+1)(x+1)$$

12. **Week12**

12.1. **Definitions:** ▶

▶ **Trivial Factorization**: n an integral domain D:
The factorization $a = bc$ is said to be **trivial** is one of b, c is a unit.
Note: Every element has many trivial factorizartion: for any unit u, we can write

$$a = u(u^{-1}a)$$

▶ **Irreducible**: $a \in D$ is said to be irreducible if it is

(1) not zero
(2) not a unit
(3) has no non-trivial factorization

Example: in $\mathbb{Z}$, 7 is irreducible, but 6 is not irreducible, because $6 = 2{\cdot}3$.

▶ **Prime ideal**: Let R be a commutative, unital ring, I an ideal of R. I is a prime ideal if

(1) $I \neq R$, and
(2) $ab \in I \Rightarrow$ either $a \in I$ or $b \in I$.

Example: Examples from $\mathbb{Z}$: $\langle 0 \rangle$ is prime:
$\langle 0 \rangle = \{0\} \neq \mathbb{Z}$
$ab \in \{0\} \Rightarrow ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$.
Non-examples in $\mathbb{Z}$:

(1) $\langle 1 \rangle$ is not prime because $\langle 1 \rangle = \mathbb{Z}$
(2) $\langle 6 \rangle$ is not prime: $2 \cdot 3 \in \langle 6 \rangle$, but $2 \notin \langle 6 \rangle$ and $3 \notin \langle 6 \rangle$

▶ **Unique factorization domain**: The integral domain D is said to have unique factorization if

(1) If $a \in D$ is not zero, not a unit, then there is some factorization $a = p_1 p_2 \cdots p_k$, $p_1, \cdots, p_k$ are all irreducible.
(2) If we have two such factorizations,

$$a = p_1 \cdots p_j = q_1 \cdots q_l$$

then $k = l$ and, after reordering the $q's$, if necessary, $p_i \sim q_i \forall i$.

$$x^3 - x = x(x-1)(x+1) = (2x-2)(\frac{1}{2}x)(x+1) = (\frac{1}{2}x)(2x-2)(x+1)$$

$$x \sim \frac{1}{2}x, \cdots$$

▶ **Principal ideal domain**: A domain D is a principle ideal domain (PID) if every ideal of D is principle.
(Principle ideals: Let R be any unital ring, and let $a \in R$. Define

$Ra = \{ra | r \in R\}$.)
Example: $\mathbb{Z}$ is a PID.
Any ideal I of $\mathbb{Z}$ is also an additive subgroup of $\mathbb{Z}$, hence cyclic, so equal to $n\mathbb{Z}$ for some $n \geq 0$. But $n\mathbb{Z} = \langle n \rangle$.

▶ **Prime element**: In an integral domain D, the element $a \in D$ is prime if

(1) $a \neq 0$
(2) a is not a unit
(3) $a|bc \Rightarrow a|b$ or $a|c$

Example: Non-example:
In $\mathbb{Z}$, 4 is not a prime:

$$4|12$$
$$4|2 \cdot 5$$

but

$$4 \nmid 2, 4 \nmid 6$$

But 5 is prime in $\mathbb{Z}$.

▶ **Proper divisor chain**: A proper divisor chain is a sequence of elements

$$a_1, a_2, a_3 \cdots$$

with

$$a_2|a_1, a_3|a_2, a_4|a_3, \cdots$$

(i.e., $a_{i+1}|a_i \forall i$)
and $a_{i+1} \not\sim a_i$.
Example:

$$75, 15, 5, 1$$

▶ **Divisor chain condition**: D satisfies the divisor chain condition if it has no infinite proper divisor chains. (D is an integral domain)
Example: In $\mathbb{R}[x]$:

$$x^3 - x, x - 1, 1$$

12.2. **Theorems: ★**

★ **Theorem relating prime ideals to integral domains:** R/I **is an integral domain** $\iff$ **I is prime**.

★ **Theorem relating irreducible elements to maximal ideals ("If** D **is a principal ideal domain, then** $\langle$**m**$\rangle$ **is maximal if and only if m is...")**: If D is a PID, then $\langle m \rangle$ is maximal iff m is irreducible.

(Addition theorems in class:)
(In $F[x]$, the ideal $\langle m \rangle$ is maximal if and only if m is irreducible.)
(Every maximal ideal is prime.)

★ **Theorem relating prime elements to irreducible elements in general**: In any integral domain, primeness implies irreducibility.

★ **Theorem relating prime elements to irreducible elements in principal ideal domains**: If D is a PID and $a \in D$ is irreducible, then a is prime. (Hence, in PID's, then concept of primeness and irreducibility are equivalent).

★ **Criteria for D to have unique factorization**: Suppose that D satisfies the divisor chain condition and in addition every irreducible element of D is prime. Then D has unique factorization.

★ **Classification of ideals in** $\mathbb{Z}$ **("**$\mathbb{Z}$ **is a...")**: $\mathbb{Z}$ has unique factorization.

★ **Theorem concerning divisor chains in** $\mathbb{Z}$ ("$\mathbb{Z}$ has no..."): $\mathbb{Z}$ satisfies the divisor chain condition and has no infinite proper divisor chains.

★ **Theorem concerning unique factorization in** $\mathbb{Z}$: $\mathbb{Z}$ has unique factorization.

★ **Classification of ideals in F[x] ("For any field** F**,** $F[x]$ **is a..."**): " If F is a field, then every ideal of $F[x]$ is principle
For any field F, $F[x]$ is a PID.

$$F[x]/\langle m \rangle$$

will be

- field if m is ireeductible
- $\backsimeq F[x]$ if $m = 0$
- $\{0\}$ if m is a unit
- not an integral domain otherwise

★ **Theorem concerning divisor chains in F[x]** ("For any field F, $F[x]$ has no..."): $F[x]$ satisfies the divisor chain condition and has no infinite proper divisor chains.

★ **Theorem concerning unique factorization in F[x]**: $F[x]$ has unique factorization.

★ **List of units of** $F[x]$: elements with degree 0

★ **Theorem relating maximal ideals to irreducible elements (in PIDs)**: the ideal $\langle m \rangle$ is maximal iff m is irreducible. ?

★ **Criterion for** $F[x]/\langle m \rangle$ **to be a field**: $F[x]/\langle m \rangle$ is a field if m is irreducible.

Last Week:

$$F[x]/\langle m\rangle$$

will be

- field if m is ireeductible
- $\backsimeq F[x]$ if $m = 0$
- $\{0\}$ if m is a unit
- not an integral domain otherwise

12.3. **Unique Factorization.**

$$12 = 2 \cdot 6, 6 = 2 \cdot 3$$

$$12 = 3 \cdot 4, 4 = 2 \cdot 2$$

$$12 = 2 \cdot 2 \cdot 3$$

$$12 = 3 \cdot 3 \cdot 2$$

$$12 = (-3) \cdot (-4), (-4) = 2 \cdot (-2)$$

$$12 = (-3) \cdot 2 \cdot (-2)$$

In $\mathbb{R}[x]$

$$x^3 - x = x \cdot (x^2 - 1), x^2 - 1 = (x - 1)(x + 1)$$

$$x^3 - x = (\frac{1}{2}x)(2x - 2)(x + 1)$$

Definition 44. *The integral domain D is said to have unique factorization if*

(1) *If $a \in D$ is not zero, not a unit, then there is some factorization $a = p_1 p_2 \cdots p_k$, $p_1, \cdots, p_k$ are all irreducible.*
(2) *If we have two such factorizations,*

$$a = p_1 \cdots p_j = q_1 \cdots q_l$$

then $k = l$ and, after reordering the $q's$, if necessary, $p_i \sim q_i \forall i$.

$$x^3 - x = x(x - 1)(x + 1) = (2x - 2)(\frac{1}{2}x)(x + 1) = (\frac{1}{2}x)(2x - 2)(x + 1)$$

$$x \sim \frac{1}{2}x, \cdots$$

Theorem 32. ***Foundamental Theorem of Arithmetic***
$\mathbb{Z}$ has unique factorization.

Goal: Prove this within a few days.

Example 75. *An Integral Domain That does not have Unique Factorization:* $\mathbb{Z}[\sqrt{-5}]$

$$\mathbb{Z}[\sqrt{-5}] = \{a + bi\sqrt{5} | a, b \in \mathbb{Z}\}$$

$$3 - 4i\sqrt{5} \in \mathbb{Z}[\sqrt{-5}]$$

Exercise: $\mathbb{Z}[\sqrt{-5}]$ is a subring of $\mathbb{C}$. So $\mathbb{Z}[\sqrt{-5}]$ is an integral domain. What are the units?
Suppose $a + bi\sqrt{5}$ is a unit, with inverse $c + di\sqrt{5}$.

$$(a + bi\sqrt{5})(c + di\sqrt{5}) = 1 + 0i\sqrt{5}$$

$$(ac - 5bd) + (ad + bc)i\sqrt{5} = 1 + 0i\sqrt{5}$$

$$ac - 5bd = 1, ad + bc = 0$$

Definition 45. *Define* $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ *by* $N(a + bi\sqrt{5}) = a^2 + 5b^2 = |a + bi\sqrt{5}|^2$

$$N(z_1 z_2) = N(z_1)N(z_2)$$

$$N(a + bi\sqrt{5})N(c + di\sqrt{5}) = 1$$

So $N(a + bi\sqrt{5}) = \pm 1$.

$$a^2 + 5b^2 = \pm 1$$

$$\Rightarrow b = 0$$

$$U(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}$$

$$6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

On the homework, show 2 is irreducible, 3 is irreducible, $1 + i\sqrt{5}, 1 - i\sqrt{5}$ is irreducible.

Question: Does $F[x]$ have unique factorization?
Answer: Yes, but it will take a while to. prove.

12.4. **Prime Elements.**

Definition 46. *In an integral domain* D*, the element* $a \in D$ *is prime if*

(1) $a \neq 0$
(2) a *is not a unit*
(3) $a|bc \Rightarrow a|b$ *or* $a|c$

Example 76. *Non-example:*
In $\mathbb{Z}$*,* 4 *is not a prime:*

$$4|12$$
$$4|2 \cdot 6$$

but

$$4 \nmid 2, 4 \nmid 6$$

But 5 *is prime in* $\mathbb{Z}$*.*

Example 77. *Non-example:*
In $\mathbb{Z}[\sqrt{-5}]$*,* 2 *is not a prime:*

$$2|(1 + i\sqrt{5})(1 - i\sqrt{5})$$

but

$$2 \nmid i\sqrt{5}, 2 \nmid i\sqrt{5}$$

Note: In $\mathbb{Z}[\sqrt{-5}]$, 2 is irreducible but not prime.
Monday: Prime elements: $p \in D$ is a prime if

(1) $p \neq 0$
(2) $p \notin U(D)$
(3) $p|ab \Rightarrow p|a$ or $p|b$

This is not equivalent in general to irreducibility ($\mathbb{Z}[\sqrt{-5}]$)

$$2|(1 + i\sqrt{5})(1 - i\sqrt{5})$$

but

$$2 \nmid (1 + i\sqrt{5}), 2 \nmid (1 - i\sqrt{5})$$

Today(Wednesday):

12.5. **Actual relationship between Primeness and Irreducible.**

Theorem 33. *In any integral domain, primeness implies irreducibility.*

Proof. Suppose p is prime. We need only show that every factorization of p is trivial.

Suppose we have a factorization

$$p = ab$$

Then $p|ab$ so either $p|a$ or $p|b$.
Case1: $p|a$ then also $a|p$. So $p \sim a$. Then $p = ua$ for some unit u. So $ab = ua$. Also $a \neq 0$ (because $p \neq 0$). (In the integral Domain, cancellation law, we can cancel a). Then $b = u$, so b is a unit.
Case 2 is similar.

□

12.6. **Principle Ideal Domains.**

Definition 47. *A domain D is a principle ideal domain (PID) if every ideal of D is principle.*

(Principle ideals: Let R be any unital ring, and let $a \in R$. Define $Ra = \{ra | r \in R\}$)

Example 78. *$\mathbb{Z}$ is a PID.*

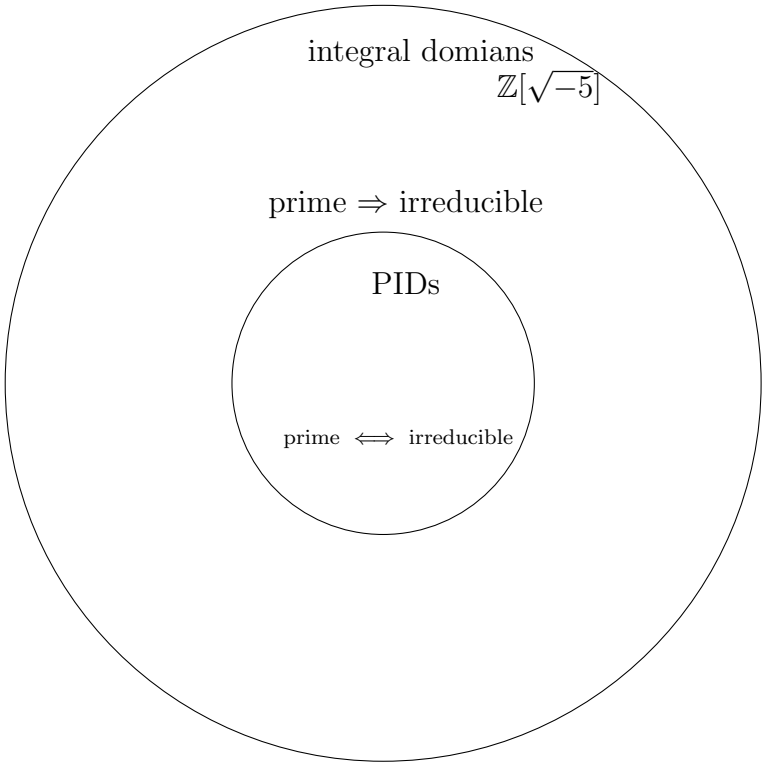
Proof. Any ideal I of $\mathbb{Z}$ is also an additive subgroup of $\mathbb{Z}$, hence cyclic, so equal to $n\mathbb{Z}$ for some $n \geq 0$. But $n\mathbb{Z} = \langle n \rangle$.

□

Example 79. *If F is any field, then $F[x]$ is a PID.*

Example 80. *Non-examples are hard to construct. We will see one in a few minutes.*

Theorem 34. *If D is a PID and $a \in D$ is irreducible, then a is prime. (Hence, in PID's, then concept of primeness and irreducibility are equivalent).*



Proof. Suppose a is irreducible.
Claim: $\langle a \rangle$ must be maximal:
$\langle a \rangle \neq D$ because a is not a unit.
Suppose $\langle a \rangle \subseteq J \subseteq D$, write $J = \langle j \rangle$
$\langle a \rangle \subseteq \langle j \rangle$, so $j|a$. Write $a = jk$.
Since a is irreducible, this factorization is trivial:
Case 1: j is a unit, then $J = \langle j \rangle = \mathrm{D}$.
Case 2: k is a unit. Then $a = jk$ so $a \sim j$.
Then $\langle a \rangle = \langle j \rangle$
So, $\langle a \rangle$ is maximal. But every maximal, ideal is a prime ideal. Thus, $\langle a \rangle$ is a prime ideal.

Suppose $a|bc$. Then $bc \in \langle a \rangle$.
Case 1: $b \in \langle a \rangle$. Then $a|b$
Case 2: $c \in \langle a \rangle$. Then $a|c$

(By hypothesis, a is irreducible, and units are not irreducible, a cannot be a unit. □

12.7. **Divisor Chain Condition.**

Definition 48. ***A proper divisor chain*** *is a sequence of elements*

$$a_1, a_2, a_3 \cdots$$

with

$$a_2|a_1, a_3|a_2, a_4|a_3, \cdots$$

(i.e., $a_{i+1}|a_i \forall i$)
and $a_{i+1} \not\sim a_i$.

Example 81. *Example from* $\mathbb{Z}$

$$75, 15, 5, 1$$

(can't extend)

$$-12, 6, -2, -1$$

(blocked now)

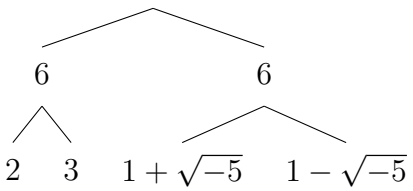
Example 82. *in* $\mathbb{R}[x]$*:*

$$x^3 - x, x - 1, 1$$

Definition 49. *D satisfies the divisor chain condition if it has no infinite proper divisor chains. (Like examples above)*

Previous Point:

$\mathbb{Z}[\sqrt{-5}]$



Last time: Prime elements divisor chain condition.

- There are no infinite proper divisor chains.
  (for some integral domains but not others).

$$70, 35, 7, 1$$

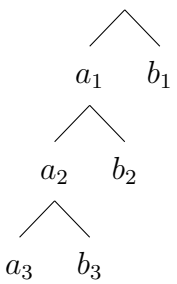
Theorem 35. *Suppose D is an integral domain and satisfies the divisor chain condition. Then, any non-zero, non-unit element has an irreducible factor.*

Proof. Suppose $a \in D$ is non-zero, not a unit.
If a has no non-trivial factorization, then a is an irreducible factor of a (because a is irreducible if $a \neq 0$, $a \neq$ unit, a has no non-trivial factorization.).
Otherwise, unit $a = a_1 b_1$, with neither factors a unit.

Then, If a is irreducible, then a_1 is irreducible factor of a.
Otherwise, $a_1 = a_2 b_2$ with neither factor a unit.

Continuing in this, either we find an irreducible factor OR we get a divisor chain $a, a_1, a_2, a_3, \cdots$, which is an infinite divisor chain.
Infinite divisor chain $\rightarrow$ prohibited by hypothesis.

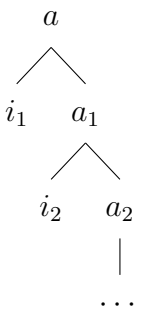
a (Keep going until get an irreducible factor).



□

Theorem 36. *If D satisfies divisor chain condition, then every non-zero, non-unit $a \in D$ has a factorization $a = i_1, i_2, \cdots i_k$ into irreducible elements.*

Proof. If a is irreducible, take $i_1 = a$, otherwise, let i_1 be an irreducible factor.
Write $a = i_1 a_1$ (here i_1 is irreducible). If a_1 is irreducible, then put $i_2 = a_1$. Otherwise $a_1 = i_2 a_2$ for i_2 irreducible.
If this goes on forever, then $a, a_1, a_2, a_3, \cdots$ is an infinite proper divisor chain, and this **does not happen**.
When the process stops, we have produced the desired factorization.



□

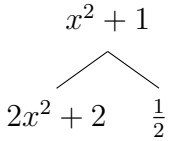
Theorem 37. *$\mathbb{Z}$ satisfies the divisor chain.*

Proof. Define $N(i) = |i|$ ($N(i)$ means the norm of integer i, $|i|$ is the absolute value of i).
This is always a non-negative integer, and if $b|a$ with $b \not\sim a$, then $N(b) < N(a)$. This cannot go on forever.

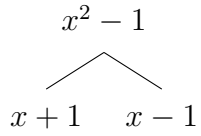
□

Theorem 38. *$F[x]$ satisfies the divisor chain condition.*
Proof is the same as for $\mathbb{Z}$, just take $N(f) = deg(f)$.

Example 83.



(This becomes a trivial factorization because $\frac{1}{2}$ is a unit, it is already irreducible),



(Degree is always getting smaller, it will become irreducible or get to degree of 1*, which is always irreducible)*

Theorem 39. $\mathbb{Z}[\sqrt{-5}]$ *does satisfy the divisor chain condition.*

Proof. (Sketch of the proof)
$N(a+bi\sqrt{5}) = a^2+5b^2$ (complex absolute value squared)

□

Theorem 40. *Suppose that* D *satisfies the divisor chain condition and in addition every irreducible element of* D *is prime. Then* D *has unique factorization.*

Proof. Suppose we have a non-zero, non-unit $a \in D$ with two factorizations into primes

$$a = p_1 p_2 \cdots p_k$$
$$= a_1 a_2 \cdots a_l$$

(p_i, a_i are irreducible (prime))
(each p is associated to each a).
$p_1|a$, so $p_1|(a_1 a_2 \cdots a_l)$
p_1 is prime and it divides $(a_1)(a_2 a_3 \cdots a_l)$, sp wither $p_1|a_1$ or $p_1|(a_2 \cdots a_l)$
continuing, we find that p_1 is a divisor of a_i for some i (it divides that product, so it will divide one of the factors)
Renumbering them as it is necessary, we can assume that $p_1|a_1$.
But, a_1 is irreducible. And p_1 is not a unit.
So, $p_1 \sim a_1$.
Write $a_1 = u_1 p_1$ (an associate is always a unit multiple)

$$p_1 p_2 \cdots p_k = a_1 a_2 \cdots a_l$$

$$p_1 p_2 \cdots p_k = u_1 p_1 a_2 \cdots a_l$$

now have a common factor that $\neq 0$, and working on an integral domain, so can cancel p_1.

$$p_2 \cdots p_k = u_1 a_2 \cdots a_l$$

p_2 cannot divide u_1 because if it did, p_2 would be an associate of u_1($p_2 \sim u_1$) $\rightarrow$ and that would mean p_2 would be a unit.
so, $p2 \nmid u_1$.
Now, as before, $p_2 \sim a_2$ (maybe after some renumbering of as).
Continue in this way, one of three things must happenL

(1) If $k < l$, then eventually we cancel everything on left-hand side and get $1 = u_1 u_2 \cdots u_k a_{k+1} \cdots a_l$.

    If this happens then a_l is a unit, because there is something 1 can multiply it by to get 1. This is a contradiction so case 1 doesn't happen.
(2) If $k > l$, we get $p_{l+1} p_{l+2} \cdots p_k = u_1 \cdots u_l$, which implies p_k is a unit which is also a contradiction. Case 2 doesn't happen.
(3) $k = l$ and theorem is proved.

□

12.8. **Problems.**

Problem 110. *The polynomial $f = x^3 + x$ has an essentially unique factorization into primes of $\mathbb{R}[x]$. Find this factorization.*

$$x^3 + x = x(x^2 + 1)$$

Problem 111. *The polynomial $f = x^3 + x$ has an essentially unique factorization into primes of $\mathbb{C}[x]$. Find this factorization.*

$$x^3 + x = x(x^2 + 1) = x(x + i)(x - i)$$

Problem 112. *"'(The domain $\mathbb{Z}[\sqrt{-5}]$)"' Recall that $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5}i \,|\, a, b \in \mathbb{Z}\}$. Show that this set is a unital subring of $\mathbb{C}$, and hence an integral domain.*

$$(a + b\sqrt{5}i)(c + d\sqrt{5}i) = 1$$
$$ac - 5bd = 1, ad + bc = 0$$
$$d = \frac{-bc}{a}$$
$$ac + \frac{5b^2c}{a} = 1$$
$$c = 1/\frac{a^2 + 5b^2}{a} = \frac{a}{a^2 + 5b^2}$$
$$d = \frac{-b}{a^2 + 5b^2}$$

When c, d are integers, $a + b\sqrt{5}i$ has inverse. And when $a^2 + 5b^2 = 1$, they are integers.
Therefore, for element $a + b\sqrt{5}i$, there can be an inverse $c + d\sqrt{5}i$. Therefore, it is a unital subring of $\mathbb{C}$.

Problem 113. *Define a function $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_{\geq 0}$ by the formula $N(z) = |z|^2$. (Here the absolute value is taken in the sense of complex numbers, i.e. $|a + bi| = \sqrt{a^2 + b^2}$.) Show that N preserves multiplication, i.e. that $N(z_1 z_2) = N(z_1)N(z_2)$.*

$$N(a + b\sqrt{5}i) = a^2 + 5b^2$$
$$N(c + d\sqrt{5}i) = c^2 + 5d^2$$
$$N((a+b\sqrt{5}i)(c+d\sqrt{5}i)) = N((ac-5bd)+\sqrt{5}(ad+bc)i) = (ac-5bd)^2+5(ad+bc)^2$$
$$= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2$$
$$N(a+b\sqrt{5}i)N(c+d\sqrt{5}i) = (a^2+5b^2)(c^2+5d^2) = a^2c^2+5a^2d^2+5b^2c^2+25b^2d^2$$
$$N((a + b\sqrt{5}i)(c + d\sqrt{5}i)) == N(a + b\sqrt{5}i)N(c + d\sqrt{5}i)$$

Problem 114. *Find all elements* $a + bi\sqrt{5} \in \mathbb{Z}[\sqrt{-5}]$ *with* $N(a + bi\sqrt{5}) = 1$.

$$a^2 + 5b^2 = 1$$

$$a, b \in \mathbb{Z}$$

$$a = \pm 1, b = 0; b = \pm 1, a = 0$$

Problem 115. *Show that an element of* $\mathbb{Z}[\sqrt{-5}]$ *is a unit if and only if it has norm one.*

If the norm is not one, $a^2 + 5b^2 > 1$. $c + d\sqrt{5}i$ *is inverse only when* c, d *are integers.*

$$c = 1/\frac{a^2 + 5b^2}{a} = \frac{a}{a^2 + 5b^2}$$

$$d = \frac{-b}{a^2 + 5b^2}$$

if $a^2 + 5b^2 > 1$, $a > 1, b > 1$ *or* $a \geq 1 \wedge b \geq 1$.
If $a > 1$, $|a| < |a^2| < |a^2 + 5b^2|$, c *cannot be an integer. If* $b > 1$, $|-b| < |5b^2| < |a^2 + 5b^2|$, d *cannot be an integer.*
if $a > 1, b > 1$, $|a| < |a^2 + 5b^2| \wedge |-b| < |a^2 + 2b^2|$, *both* c *and* d *cannot be an integer.*

Problem 116. *Show that in the ring* $\mathbb{Z}[\sqrt{-5}]$, *the factorization* $a = bc$ *is non-trivial if and only if* $N(b) < N(a)$ *and* $N(c) < N(a)$.

if $N(b) = N(a)$, $N(c) = 1$, *which means that* c *is a unit. Then* $a = bc$ *is a trivial factorization.* $N(b) > a$ *cannot happen.*

Problem 117. *Show that* $\mathbb{Z}[\sqrt{-5}]$ *has no elements of norm* 2. *"(Hint:* $N(a + bi\sqrt{5}) = a^2 + 5b^2$, *and both* a *and* b *are integers.)"*

If it has norm 2*:*

$$a^2 + 5b^2 = 2$$

Then

a^2	$5b^2$
2	0
0	2
1	1

In any cases, a *or* b *cannot be integer.*

Problem 118. *Show that* $\mathbb{Z}[\sqrt{-5}]$ *has no elements of norm* 3.

a^2	a	$5b^2$	b
3	$\sqrt{3}$	0	0
0	0	3	$\sqrt{3}$
2	$\sqrt{2}$	1	1
1	1	2	$\sqrt{2}$

Problem 119. *Calculate the norms of the elements* $2, 3, 1 + i\sqrt{5}$, *and* $1 - i\sqrt{5}$.

$$4, 9, 6, 6$$

Problem 120. *Show that all four of the elements referenced in the previous problem are irreducible in* $\mathbb{Z}[\sqrt{-5}]$.

$$4 = 2 * 2, 9 = 3 * 3, 6 = 2 * 3$$

No elements of norm 2 *or* 3, *they only have trivial factorization.*

Problem 121. *Show that none of the elements referenced above is prime.*

They are not zero, not unit (only with norm 1 has unit)
However,

$$2|6$$

$$6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$$

$$2 \nmid (1 + \sqrt{5}i), 2 \nmid (1 - \sqrt{5}i)$$

*(*2 *only has trivial factorization)*
Same thing for 3 *and* $1 + i\sqrt{5}$ *(*$6 = 2 \cdot 3$*)*

Problem 122. *Show that* $\mathbb{Z}[\sqrt{-5}]$ *does "not" have unique factorization.*

Not every irreducible elements are prime.

Problem 123. *Show that* $\mathbb{Z}[\sqrt{-5}]$ *"does" satisfy the divisor chain condition. "(Hint: think about norms in a proper divisor chain.)"*

Looking at the norm, $a = bc$, $N(b) < N(a), N(c) < N(a)$. *continue factorizing the next one. The norm is getting smaller and the process cannot go on forever.*

Problem 124. *Show that $\mathbb{Z}[\sqrt{-5}]$ must contain at least one non-principal ideal.*

An ideal I is a left and right ideal (if $i \in I$ and $r \in R$ then also $ri \in I$). A principle ideal is $Ra = \{ra | r \in R\}$.

If it contains no non-principle ideal, then all I can be written as $Ra = \{ra | r \in R\}$, which means that every element in I can be written as ra (has non-trivial factorization).

If we have an ideal containing both 2 and 3,then $I = \langle 2, 3\rangle = \{2a + 2b\sqrt{5}i | a, b \in \mathbb{Z}\} \cup \{3a + 3b\sqrt{5}i | a, b \in \mathbb{Z}\}$

We are unable to write all elements as ra, because we cannot choose a correct a.

Both 2 and 3 are irreducible and have only trivial factorization. For any elements in $\{2a + 2b\sqrt{5}i | a, b \in \mathbb{Z}\}$, we can only choose $a = 2$, however, we cannot write any elements in $\{3a + 3b\sqrt{5}i | a, b \in \mathbb{Z}\}$ as $r \cdot 2$.

Problem 125. *Consider the ideal $J = \left\langle 2, 1 + i\sqrt{5}\right\rangle = \{2(a + bi\sqrt{5}) + (1 + i\sqrt{5})(c + di\sqrt{5}) \,|\, a, b, c, d \in \mathbb{Z}\} = \{(2a + c - 5d) + (2b + c + d)i\sqrt{5} \,|\, a, b, c, d \in \mathbb{Z}\}$. Show that $2 \in J$ and $1 + i\sqrt{5} \in J$ but $1 \notin J$. "(Hint: to show that $1 \notin J$, work with the last-given description of the elements of J. In order for the coefficient of $i\sqrt{5}$ to vanish, c and d must both be even or both odd. In either case, what is the parity of $2a + c - 5d$?)"*

$$a = 1, b = c = d = 0, 2(a + bi\sqrt{5}) + (1 + i\sqrt{5})(c + di\sqrt{5}) = 2$$

$$c = 1, a = b = d = 0, 2(a + bi\sqrt{5}) + (1 + i\sqrt{5})(c + di\sqrt{5}) = 1 + i\sqrt{5}$$

If $1 \in J$, then $1 = (2a + c - 5d) + (2b + c + d)i\sqrt{5}$

$$2a + c - 5d = 1$$

$$2b + c + d = 0$$

$$c = 1 + 5d - 2a$$

$$2b + c + d = 2b + 1 + 5d - 2a + d = 2b + 6d - 2a + 1$$

$$= 2(b + 3d - a) + 1$$

It has to be an odd number, impossible to be 0. $1 \notin J$.

Problem 126. *Show that the ideal J is "not" principal. "(Hint: if it were principal, say $J = \langle g \rangle$, then the generator g would need to be a common divisor of 2 and $1 + i\sqrt{5}$. But these are irreducibles and are not associates of one another. So what are their common divisors?)"*

Both 2 and $1+i\sqrt{5}$ are irreducible and have only trivial factorization. We can write them as $2 = ab$, $1 + i\sqrt{5} = ac$ iff

$$2 \sim 1 + i\sqrt{5}$$

However

$$u(1 + i\sqrt{5}) = \pm(1 + \sqrt{5}) \neq 2, \forall u \in U(\mathbb{Z}[\sqrt{-5}\} = \{1, -1\}$$

Problem 127. *"'(Optional; a domain with an infinite divisor chain)"' This and all following exercises require some knowledge of complex analysis and are thus optional. In these exercises, if you choose to attempt them, you will construct an example of an infinite proper divisor chain. To begin with, let R denote the set of functions from $\mathbb{C}$ to $\mathbb{C}$ which are complex-analytic at every point. Using the properties of complex derivatives, show that R is a unital ring under pointwise addition and multiplication.*

Condition for the function to be complex-analytic:

$$\frac{\partial f}{\partial \bar{z}} = 0, \frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}$$

First of all, it is a ring. For any complex number on $f(x, y) = u(x, y) + iv(x, y)$, it's an abelian group under addition and associative under multiplication (all complex numbers).

Because it is complex-analytic everywhere, it is holomorphic there is no poles on the function. It has an multiplicative identity $1_{\mathbb{C}} = 1$, $1 \cdot f(x, y) = f(x, y)$.

To find the inverse, there are some $x = x_1, y = y_1$:

$$f(x_1, y_1)f(x_2, y_2) = 1$$

$$(u(x_1, y_1) + iv(x_1, y_1))(u(x_2, y_2) + iv(x_2, y_2)) = 1$$

$$(u(x_1, y_1) + iv(x_1, y_1))\frac{1}{u(x_1, y_1) + iv(x_1, y_1)} = 1$$

$$\frac{1}{u(x_1, y_1) + iv(x_1, y_1)} = \frac{u(x_1, y_1) - iv(x_1, y_1)}{(u(x_1, y_1) + iv(x_1, y_1))(u(x_1, y_1) - iv(x_1, y_1))}$$

$$= \frac{u(x_1, y_1) - iv(x_1, y_1)}{u(x_1, y_1)^2 + v(x_1, y_1)^2}$$

$$= \frac{u(x_1, y_1)}{||f(x_1, y_1)||} - \frac{v(x_1, y_1)}{||f(x_1, y_1)||} i$$

There are some x_2, y_2 *such that* $u(x_2, y_2) = \frac{u(x_1,y_1)}{||f(x_1,y_1)||}$, $v(x_2, y_2) = -\frac{v(x_1,y_1)}{||f(x_1,y_1)||}$, *because the function is holomorphic.*

Problem 128. *Show that a non-constant element of* R *can vanish at only countably many points. "(Hint: this is the hardest exercise of the whole series. You will need to use the identity theorem together with the fact that* $\mathbb{C}$ *is a second-countable topological space.)"*

Problem 129. *Show that* R *is an integral domain. "(Hint: if* $fg = 0$ *then either* f *or* g *must vanish at uncountably many points.)"*

Problem 130. *Show that a unit of R cannot have any zeros. "(Hint: if f has a zero of order d at $z = z_0$, then $1/f$ has a pole of order d at $z = z_0$.)"*

Problem 131. *Define a function $f_n : \mathbb{C} \to \mathbb{C}$ by the formula $f(z) = \sin(z)/\prod_{k=1}^{n}(z - ki\pi)$. Show that f_n has only removable singularities and thus has a unique extension to an element of R (which we shall also denote by f_n).*

Problem 132. *Describe the zeros of f_n.*

Problem 133. *Show that f_n/f_{n+1} has only removable singularities, and thus $f_{n+1} \mid f_n$.*

Problem 134. *Show that $f_{n+1} \not\sim f_n$. "(Hint: use the principle, which you proved above, that a unit of R cannot have any zeros.)"*

Problem 135. *Conclude that $(f_1, f_2, f_3, \dots)$ is an infinite proper divisor chain in R.*

13. **Week13**

.

13.1. **Procedures.** .

▶ Sieve of Eratosthenes (for integers):

▶ Sieve of Eratosthenes (for polynomials with coefficients in a finite field):

▶ Procedure to factor polynomials over $\mathbb{C}$:

- rout-finding is enough - if f is not constant. Then it has a root. ("Fundamental theorem of algebra"0
- Newton's method can find roots. ★
- Every irreducible has degree 1.

▶ Procedure to factor polynomials over $\mathbb{R}$:

- If a is a real root then $x - a$ is a factor.
- Otherwise if $a, \bar{a}$ form a conjugate pair of roots, then

$$((x-a)(x-\bar{a}))|f$$

$$((x-a)(x-\bar{a})) = x^2 - (a+\bar{a})x + a\bar{a} \in \mathbb{R}[x]$$

- Every irreducible has degree 1 or 2.

Last time: If D satisfies divisor chain condition and in which every irreducible element is prime, then D has unique factorization.

13.2. **Techniques of factorization.** Problem: given $f \in F[x]$, find "the" prime factorization $f = p_1 \cdots p_k$ (p_i is prime).

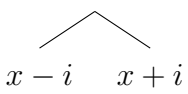
Remark 1: There can bo no completely general technique, because answers are field-dependent.

Example 84. *Factor x^2+1 over $\mathbb{R}$.*
x^2+1 is irreducible: degree is ≤ 3 and it has no roots.

Example 85. *Factor x^2+1 over $\mathbb{C}$.*

$$f(x0 = x^2 + 1$$
$$f(i) = i^2 + 1 = 0$$

so $x - i$ must be a factor.



(As long as there is a root, we can get linear factor.

- Some general techniques
- Some field-specific techniques

13.2.1. ***General techniques***.

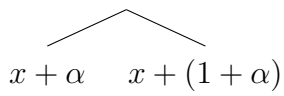
(1) If we can find one proper divisor of f, say $g_1|f$, then we can find another by long division:
divide f by g, and set $g_2 = q$.
(2) Factor Theorem: If we can find a root $a \in F$ (i.e. $f(a) = 0$), then $x - a$ is a factor.

Example 86. $GF(4) = \{0, 1, \alpha, 1+\alpha\}$.
$\alpha^2 + \alpha + 1 = 0$
$\alpha^2 = \alpha - 1 = 1 + \alpha$

Problem: Factor

$$x^2 + x + 1$$

over $GF(4)$.
We know that α is a root, so $x - \alpha$ is a factor.



Example 87.

$$x^4 + 1$$

over $\mathbb{R}$.
No real roots - no linear factors.
Claim: $x^2 - \sqrt{2}x + 1$ *is a factor.*

$$\begin{array}{ccc} & x^4+1 & \\ \swarrow & & \searrow \\ x^2 - \sqrt{2}x + 1 & & x^2 + \sqrt{2}x + 1 \end{array}$$

13.2.2. ***Field-specific techniquws***. Over $\mathbb{C}$, factorization is "easy". Every non-constant $f \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.(proof requires analysis).("Fundamental theorem of algebra")
Warning: This theorem is false for $\mathbb{Q}[i] - \{r + si | r, s, \in \mathbb{Q}\}$. This shows that root-finding is enough:

(1) Find a root a of f.
(2) Factor $f = (x - a)q$.
(3) Repeat on q.

Example 88. *Factor* $x^4 + 1$ *over* $\mathbb{C}$.

$$x^4 = -1$$
$$4arg(x) = 180 + 360k(degrees)$$
$$arg(x) = 45 + 90k$$
$$z = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$
$$x^4 = (x - z)(x - iz)(x + z)(x + iz)$$

Roots can be found using Newton's method.
Over $\mathbb{R}$: to factor $f \in \mathbb{R}[x]$

(1) Find a complex root $a \in \mathbb{C}$,
(2) The cinjugate $\bar{a}$ will also be a root.
(3) This, $x - a$ and $x - \bar{a}$ are both linear factors in $\mathbb{C}[x]$

$$(x - a)(x - \bar{a}) = x^2 - (a + \bar{a})x + a\bar{a}$$

(real and real for $a + \bar{a}$ and $a\bar{a}$)

(Before Wednesday class) In a commutative ring R, $\langle a_1, a_2, \cdots, a_k \rangle$ $= \{r_1a_1 + r_2a_2 + \cdots + r_ka_k | r_1, \cdots, r_k \in R\}$.
in $\mathbb{Z}[x], \langle \alpha, x \rangle = \{\alpha f_1 + x f_2 | f_1, f_2 \in \mathbb{Z}[x]\}$.
Monday class:
Fact: $F[x]$ has unique factorization.

- if $f(a) = 0$, then $(x - a)|f$, long division gives $f = (x - a)q$.

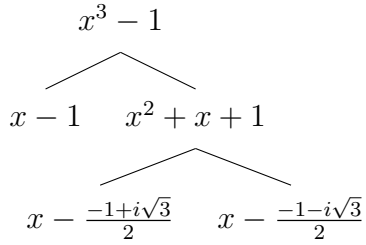
- in general, if $g_1|f$ then we get a factorization $f = g_1 g_2$ by long division.
- over $\mathbb{C}$:
  - rout-finding is enough - if f is not constant. Then it has a root. ("Fundamental theorem of algebra"0
  - Newton's method can find roots. ★
  - Every irreducible has degree 1.
- over $\mathbb{R}$:
  - If a is a real root then $x - a$ is a factor.
  - Otherwise if $a, \bar{a}$ form a conjugate pair of roots, then

$$((x-a)(x-\bar{a}))|f$$

$$((x-a)(x-\bar{a})) = x^2 - (a+\bar{a})x + a\bar{a} \in \mathbb{R}[x]$$

  - Every irreducible has degree 1 or 2.

Example 89. *Factor* $x^3 - 1$ *over* $\mathbb{R}$



Over $\mathbb{Q}$, factorizationis much harder than $\mathbb{C}$ or $\mathbb{R}$.

- $\mathbb{Q}[x]$ has irreducibles i nevery degree:
  If p is prime and n is arbitrary, $x^n - p$ is irreducible over $\mathbb{Q}$.
  Proof uses **Eisenstein's criterion**.

Example 90. *irreducible*
$$\begin{cases} x^2 - 2 \\ x^3 - 2 \\ x^4 - 2 \end{cases}$$

- But factorization in $\mathbb{Q}[x]$ is a solved problem.
- Slow algorithm - **Kronecker's Method. (c. 1900)**
  Overwhelms computers in moderate degree.
- Fast algorithm - **LLL algorithm (c. 1975)**

(All above (Factorization over $\mathbb{Q}$ works over algebraic number field)

13.3. **Finite Fields.** .
Such as

$$\mathbb{Z}_p, GF(4), GF(8), etc$$

(can still be used for information storage - see coding theory and especially linear codes. Like Ascii.)

- Slow algorithm - study in class
- Fast algorithm (need to study by myself!!!) **Google "Factorization over finite fields"**

First problem is to recognize irreducible polynomials. We will use the **Siere of Eratosthenes**

13.3.1. ***Siere of Eratosthenes.*** in $\mathbb{Z}$:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 \cdots 20$$

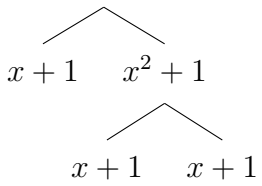
in $\mathbb{Z}_2[x]$:

$$1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$$

$$x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1$$

(Using division algorithm to see if something is divisible by x, and the next black, and the next black)
(See if something is a root)
For general polynomial:
If f is a general polynomial of degree d, we just test it for divisibility by all irreducibles of degree $< d$

Example 91. x^3+x^2+x+1 *Then repeat the procedure. If it is*

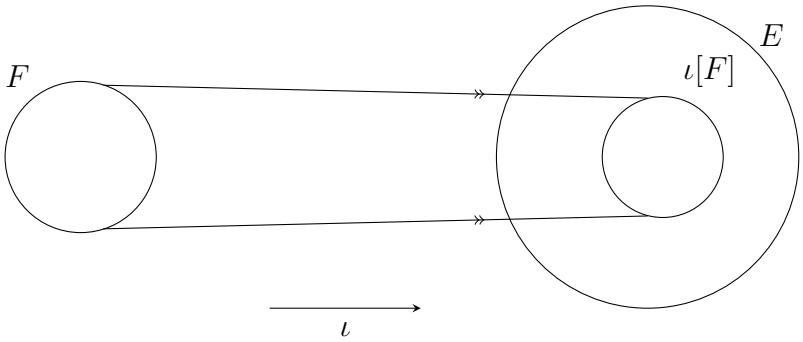


divisible by some irreducible items.

On Wednesday:
Factorization in $F[x]$.
$\mathbb{Q}$ (algebraic number fields)
$\mathbb{R}$
$\mathbb{C}$
(comes down to root-finding.
Finite fields -Sieve of Eratosthenes.
Also much faster methods: Nierreiter: Finite Fields and their application.

Today:
Did Hippasus really need to die?

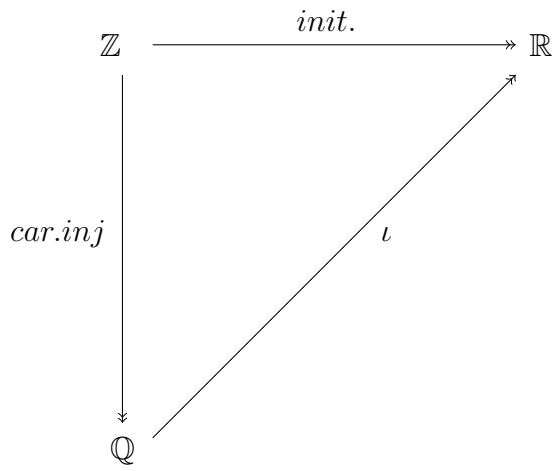
Definition 50. *A field extension is a triple (F,E,ι) where F and E are fields, and $\iota : F \to E$ is a monomorphism.*
F is called the base field, E is called the extension field, and ι is the injection.



$\iota(F)$ is a copy of F, and E is an extension fron $\iota(F)$.

Example 92. $\mathbb{Q} \to \mathbb{R}$
Take $F = \mathbb{Q}$, $E = \mathbb{R}$.
$\mathbb{Z} \to (init)\mathbb{R}$ *(*$1 \to 1.00000\cdots$*)*
$\mathbb{Z} \to (car, inj)\mathbb{Q}$
$\mathbb{Q} \to (\iota)\mathbb{R}$

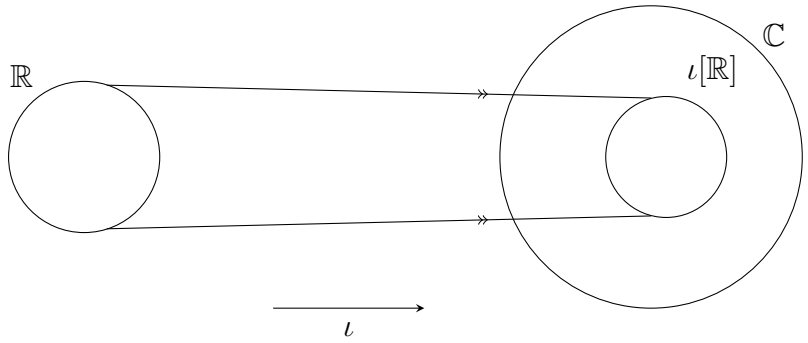
$$\iota(\frac{a}{b} = (a.000000\cdots)/(b.00000\cdots)$$



Example 93. $\mathbb{R} \to \mathbb{C}$.

$$F = \mathbb{R}$$
$$E = \mathbb{C}$$
$$\iota(a) = a + 0i$$

(Real is the real axis in complex plane).



Example 94. $\mathbb{Z}_2 \to GF(4)$

$$F = \mathbb{Z}_2$$
$$E = GF(4) = \{0, 1, \alpha, 1 + \alpha\}(\alpha^2 = 1 + \alpha$$

Example 95. $\mathbb{Q} \to \mathbb{Q}[\sqrt{2}]$

$$F = \mathbb{Q}$$
$$E = \mathbb{Q}[\sqrt{2}] = \mathbb{Q}[x]/\left\langle x^2 - 2 \right\rangle$$

Remark: x^2-2 *is irreducible because its degree is* ≤ 3 *and it has no roots in* $\mathbb{Q}$.
$\mathbb{Q}[x]/\langle x^2-2\rangle$ *is a field.*

$$\iota(a) = a + 0\alpha$$
$$(\alpha = x + \langle x^2-2\rangle)$$

Usually people name x *(or* α*? I forgot) as* $\sqrt{2}$.

$$(\sqrt{2} = x + \langle x^2-2\rangle)$$
$$\sqrt{2}^2 - 2 = 0$$
$$(\sqrt{2})^2 = 2$$

It is a reasonable name.
"Symbolic Computation".

Theorem 41. ***Kronecker's Theorem***
Suppose F *is a field, and* $F \in F[x]$ *is a non-constant polynomial with coefficient in* F. *Then there exists a field extension* (F, E, ι) *and an element* $\alpha \in E$ *with* $f(\alpha) = 0$.

$$F = \mathbb{Q}, x^2 - 2 = 0$$

Proof. Since f is not constant, it is not a unit of $F[x]$ (if a unit, degree will be ≥ 0, field has no zero-divisors), and $f \neq 0$, write

$$f = f_1 f_2 \cdots f_k$$

($f_i \in F[x]$ is irreducible)
put

$$E = F[x]/\langle f_1\rangle$$

This is a field.
Put

$$\alpha = x + \langle f_1\rangle$$

Then $f_1(\alpha) = 0$ (this is a theorem).
So

$$f(\alpha) = f_1(\alpha) f_2(\alpha) \cdots f_k(\alpha) = 0$$
$$a \in F, \iota(a) = a + 0\alpha + 0\alpha^2 + \cdots + 0\alpha^{def(f_1)-1}$$

Exercise: $\iota : F \to E$ is a monomorphism. □

Example 96. $F = \mathbb{Q}, f = x^2 - 2$
$f = (x^2-2)$ *(irreducible)*

$$E = \mathbb{Q}[x]/\langle x^2-2\rangle$$

Example 97. $F = \mathbb{Q}, f = x^4 - 5x^2 + 6.$

$$f = (x^2 - 3)(x^2 - 2)$$
$$E = \mathbb{Q}[x]/\left\langle x^2 - 3 \right\rangle = \mathbb{Q}[\sqrt{3}] = \{r + s\sqrt{3} | r, s \in \mathbb{Q}\}$$
$$f(\sqrt{3}) = (\sqrt{3})^4 - 5(\sqrt{3})^2 + 6$$
$$= 0$$

(No uniqueness, we can also use a different extension field with another factor.)

Example 98. $F = \mathbb{Q}, f = x^3 + x$

$$f = x^3 + x = x(x^2 + 1)$$
$$E = \mathbb{Q}[x]/\left\langle x \right\rangle = \{a | a \in \mathbb{Q}\} \simeq \mathbb{Q}$$

(Already factored)

$$\alpha = x + \langle x \rangle = 0 + \langle x \rangle$$

13.4. **Problems.** .

Problem 136. *Skim the introduction to https://en.wikipedia.org/wiki/Factorization_of_polynom the Wikipedia article on polynomial factorization so you will know where to find search terms when you one day need to know how to factor high-degree polynomials.*

Problem 137. *Working over $\mathbb{Z}_2$, factor the polynomial x^3+1 into irreducibles. "(Hint: first look for roots and pull out the corresponding linear factors by long division.)".*

$$x^3+1$$
$$1^3+1=2=0$$
$$f(1)=0$$

$(x-1)=(x+1)$ *is a factor. Also,* $x+1$ *has degree* 1*, it is irreducible.*

$$x^3+1=(x+1)(x^2+x+1)$$

(x^2+x+1) *has no root in* $\mathbb{Z}_2$*, therefore,* x^2+x+1 *is irreducible.*

Problem 138. *Repeat the previous exercise for x^4+1 and for x^5+1. "(Hint: the hardest part will be deciding whether $x^4+x^3+x^2+x+1$ can be factored as the product of two quadratics. But for this, you can make a list of all irreducible quadratics and test for divisibility by each in turn.)".*

$$x^4+1=(x+1)(x+1)(x^2+x+1)$$
$$x^5+1=(x+1)(x^4+x^3+x^2+x+1)$$

Some irreducible element:

$$1,x,x+1,x^2+x+1,x^3+x+1,x^3+x^2+1,x^4+x+1$$

$(x^4+x^3+x^2+x+1)$ *is irreducible.*

Problem 139. *Working over $\mathbb{Z}_3$, find all irreducible polynomials of degree two. "(Hint: you do not need the Sieve; you just need to find quadratics that have no roots.)".*

$$0^2=0,1^2=1,2^2=1$$
$$x^2+1,2x^2+2,2x^2+x+1,2x^2+2x+1,2x^2+2x+2$$

Problem 140. *Construct a field with nine elements.*

$$\{ax+b|a,b\in\mathbb{Z}_3\}$$

14. **Week14**

.

14.1. **Definitions.** .

►Splitting field (of a non-constant polynomial $f \in F[x]$): Suppose $f \in F[x]$ is non-constant, and $F \to E$ is a field extension. We say that f splits over E if f can be written as a product of linear factors in $E[x]$.
We say $F \to E$ is a splitting field for f if

(1) The polynomial f splits over E, and
(2) The extension $F \to E$ is generated by roots of f, i.e. the smallest subfield of E containing (the image of) F and all of the roots of f is E itself.

Example:
$f = x^2-4$ splits over $\mathbb{Q}$, since $f = (x-2)(x+2)$. By contrast, $g = x^2-5$ does not split over $\mathbb{Q}$.

► Isomorphism (of field extensions): Suppose (F, E_1, ι_1) and (F, E_2, ι_2) are extensions of the same base field. We say that these extension are isomorphic if there exists a field isomorphism $\phi : E_1 \to E_2$ with $\phi \circ \iota_1 = \iota_2$.
Example:
$F = \mathbb{Q}$, $E_1 = \mathbb{Q}[x]/\langle x^2 - 2\rangle$ with $\iota(\alpha) = (\alpha + 0x + 0x^2 + \cdots) + \langle x^2 - 2\rangle$ (Send the rational number α to the coset of the constant polynomial with value α).
$E_2 = \{r + s\sqrt{2} | r, s \in \mathbb{Q}\}$ ($\sqrt{2}$ denotes the positive real number whose square is 2, E_2 is a subset over $\mathbb{R}$.) E_2 is a subfield of $\mathbb{R}$ (To prove every element is a unit, write $\frac{1}{r+s\sqrt{2}}$ in the form of $\frac{r}{r^2-2s^2} + \frac{-s}{r^2-2s^2}\sqrt{2}$).
Define $\iota_2 : \mathbb{Q} \to E_2$ by $\iota_2(r) = r + 0\sqrt{2}$.
$(\mathbb{Q}, E_1, \iota_1)$ and $(\mathbb{Q}, E_2, \iota_2)$ isomorphic field extensions.
Define a map ψ: $\mathbb{Q}[x] \to \mathbb{R}$ by the formula $\psi(a_0 + a_1x + a_2x^2 + a_3x^3 \cdots) = (a_0 + 2a_2 + 2^2a_4 + \cdots) + (a_1 + 2a_3 + 2^2a_5 + \cdots)\sqrt{2}$. We can see $im(\psi) = E_2$. ψ is a unital ring homomorphism.
$ker(\psi)$ is an ideal of $\mathbb{Q}[x]$ that contains $x^2 - 2$ (because $\psi(x^2 - 2) = 2 \cdot 1 - 2 = 0$, and $ri \in I \Rightarrow r(x^2 - 2) = 0$)
Applying Fundamental Theorem on Homomorphism, we can get a homomorphism $\hat{\psi} : E_1 \to \mathbb{R}$ whose image is E_2, restricting the codomain gives an isomorphism from E_1 to E_2.
$\hat{\psi}(\iota_1(r)) = \hat{\psi}((r + 0x + \cdots) + \langle x^2 - 2\rangle) = r + 0\sqrt{2} = \iota_2(r)$. $\hat{\psi}$ is an

isomorphism of field extensions.

▶ $\mathbf{NS_F(f)}$: Suppose $f \in F[x]$ is not constant. The non-split part of f over F, denoted $NS_F(f)$, is the product of the non-linear irreducible factors of f in $F[x]$. (If there are no such factors, then by convension we take the empty product to be 1).
Example: For $NS_{\mathbb{Q}}(x^5-3x^3+x)$. $x^5-3x^3+x = x(x-2)(x+2)(x^2+1)$. $NS_{\mathbb{Q}}(x^5-3x^3+x) = x^2+1$.

▶Automorphism (of a field extension): Let (F, E, ι) be a field extension. An automorphism of (F, E, ι) is an isomorphism from (F, E, ι) to itself, i.e. a unital ring isomorphism $\phi : E \to E$ satisfying $\phi \circ \iota = \iota$.
Example:
Define $\iota : \mathbb{R} \to \mathbb{C}$ by the function $\iota(a) = a + 0i$ (it is true that ι is a unital ring monomorphism, so that $(F, E\iota)$ is a legitimate field extension. Define $\gamma : \mathbb{C} \to \mathbb{C}$ by the formula $\gamma(a + bi) = a - bi$. $\gamma(\iota(a)) = \gamma(a + 0i) = a - 0i = \iota(a)$. So indeed $\gamma \circ \iota = \iota$ and γ is a legitimate automorphism of the extension $(\mathbb{R}, \mathbb{C}, \iota)$. ($\gamma$ is the reflection over real axis in the complex plane, ι is the real axis. Reflection real over real axis (when complex part is 0) would not change anything.

▶Gal(F, E, ι) (the "Galois group" of the extension (F, E, ι)): the group of automorphisms of the field extension (F, E, ι) is called its Galois Group, and is denoted $Gal(F, E, \iota)$ (or $Gak(F \to E)$ or $Gal_F(E)$).
Example: $Gal(\mathbb{R}, \mathbb{C}, \iota) = \{e, \gamma\}$ is a two-element group and is isomorphic to $\mathbb{Z}_2$.
(e: identity map $\mathbb{C} \to \mathbb{C}$, conjugation map $\gamma : \mathbb{C} \to \mathbb{C}$)
$\psi(i) = i$ (fix real numbers). $\psi(a+bi) = \psi(a)+\psi(b)\psi(i) = a+bi$, $\psi = e$
$\psi(i) = -i$, then $\psi(a + bi) = a - bi$, $\psi = \gamma$. (Then prove with Sudoku game table).

▶ $\phi(H)$ (the "fixed field" of the subgroup $H \leq$ Gal(F, E, ι)): Put $G = Gal(F \to E)$, and suppose H is a subgroup of G. The fixed field of H is the set of all points of E that are left fixed by every element of H. In symbols: $\phi(H) = \{e = E | \forall h \in H, h(e) = e\}$ (the set $\phi(H)$ is eventually a subset of E, H is a subgroup of G, and $\phi(H)$ is a subfield of E that contains the image of F, i.e. it is a so-called subextension of (F, E, ι))
Edxample: $G = \{e, \gamma\}$. This has two subgroups $\{e\}, \{e, \gamma\}$ ($\gamma \circ \gamma = e$).
$\phi(\{e\}) = \mathbb{C}$ (every complex numbers are fixed by e).
$\phi(\{e, \gamma\}) = \mathbb{R}$ ($a + bi = a - bi$ iff $b = 0$, so only real numbers are fixed by γ)

▶ The Galois Correspondence: ϕ itself (from previous definition) from the set of subgroups of $Gal(F, E, \iota)$ to the set of subextensions of (F, E, ι). This function is called Galois Correspondence.

14.2. **Theorems.** .

★ Theorem on existence and uniqueness of splitting fields: Suppose F is a field and $f \in F[x]$ is a non-constant polynomial with coefficient in F. Then f has a splitting field. Moreover, splitting field are unique up to isomorphism of field extensions.
Example: $f = x^4 - 5x^2 + 6$ over $\mathbb{Q}$.
$E_1 = \mathbb{Q}[x]/\langle x^2 - 2\rangle$ and we denote satndard generator $x + \langle x^2 - 2\rangle$ by α. Factor f over E_1, $f = (x - \alpha)(x + \alpha)(x^2 - 3)$, E_1 is not a splitting field.
$E = E_1[x]/\langle x^2 - 3\rangle$ and denoted standard generator $x + \langle x^2 - 3\rangle$ by β. $f = (x - \alpha)(x + \alpha)(x - \beta)(x + \beta)$, f splits over E.
$E = \{b_0 + b_1\beta | b_0, b_1 \in E_1\}$, $E_1 = \{a_0 + a_1\alpha | a_0, a_1 \in \mathbb{Q}\}$, then $E = \{(a + b\alpha) + (c + d\alpha)\beta | a, b, c, d \in \mathbb{Q}\} = \{a + b\alpha + c\beta + d\alpha\beta | a, b, c, d \in \mathbb{Q}\}$
★ Fundamental Theorem of Galois Theory : Galois Correspondence is bijective.

14.3. **Problems.**

Problem 141. *Using the Sieve of Eratosthenes (or any other suitable method, such as root-searching), show that the polynomial x^3+x+1 is irreducible over $\mathbb{Z}_2$.*

Problem 142. *Show that the quotient ring $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ is a field. (It is usually denoted $GF(8)$.)*
Z_2 is a field, x^3+x+1 is irreducible, therefore, the quotient ring is a field.

Problem 143. *How many elements does $GF(8)$ have?*
Answer: 8

Problem 144. *List the elements of $GF(8)$ explicitly.*

Similar to $GF(4)$.

$$F[x]/\langle m\rangle = \{f+\langle m\rangle \,|def(f) < deg(m)\}$$
$$\mathbb{Z}_2[x]/\left\langle x^3+x+1\right\rangle = \{f+\left\langle x^3+x+1\right\rangle \,|def(f) < 3 \leq 2\}$$
$$= \{a+bx+cx^2+\left\langle x^3+x+1\right\rangle \,|a,b,c \in \mathbb{Z}_2\}$$

f can be

$$0, 1, x, 1+x, x^2, x^2+1, x^2+x, x^2+x+1$$

then we can make

$$0+\left\langle x^3+x+1\right\rangle = 0$$
$$1+\left\langle x^3+x+1\right\rangle = 1$$
$$x+\left\langle x^3+x+1\right\rangle = \alpha$$
$$1+x+\left\langle x^3+x+1\right\rangle = 1+\alpha$$
$$x^2 = x^2+\left\langle x^3+x+1\right\rangle = (x+\left\langle x^3+x+1\right\rangle)(x+\left\langle x^3+x+1\right\rangle) = \alpha^2$$
$$x^2+1+\left\langle x^3+x+1\right\rangle = \alpha^2+1$$
$$x^2+x+\left\langle x^3+x+1\right\rangle = \alpha^2+\alpha$$
$$x^2+x+1+\left\langle x^3+x+1\right\rangle = \alpha^2+\alpha+1$$

When we do multiplication in the table, if we get something like $\alpha^2\cdot\alpha = \alpha^3$, then we do $\alpha^3 = x^3+\langle x^3+x+1\rangle = x+1+\langle x^3+x+1\rangle$ because $(x^3)/(x^3+x+1), r = x+1$

Problem 145. *Define a function $\phi : GF(8) \to GF(8)$ by the formula $\phi(x) = x^2$. Show that ϕ is a unital ring homomorphism. "(Hint: to prove that it preserves addition, use the Freshman's Dream.)"* $\phi(x_1+x_2) = (x_1+x_2)^2 = x_1^2+2x_1x_2+x_2^2 = x_1^2+x_2^2 = \phi(x_1)+\phi(x_2)$ $\phi(x_1x_2) = (x_1x_2)^2 = x_1^2x_2^2 = \phi(x_1)\phi(x_2)$ $\phi(1) = 1^2 = 1$

Problem 146. *Compute* $\ker(\phi)$.
$\ker(\phi) = 0$ *(field has no zero divisor)*

Problem 147. *Show that* ϕ *is bijective, and hence an isomorphism from* $GF(8)$ *to itself. (It is usually called the "Frobenius automorphism".)*
Diagram or field rules.

Problem 148. *Make a table of values for* ϕ. *"(This is not as tedious as it appears at first. Remember the Freshman's Dream!)"*

Problem 149. *Now define* $\iota : \mathbb{Z}_2 \to GF(8)$ *by the usual formula* $\iota(a) = a + 0\alpha + 0\alpha^2$, *so that* $(\mathbb{Z}_2, GF(8), \iota)$ *is a field extension. Show that* ϕ *is an automorphism of this extension.*
ϕ *is a unital ring homomorphism and also it is bijective, therefore, it is a unital ring isomorphism. Then* $\phi \circ \iota = \iota$. *It is an sutomorphism.*

Problem 150. *It is possible to show that* ϕ *generates the whole of* $\mathrm{Gal}(\mathbb{Z}_2, GF(8), \iota)$. *Taking this for granted, make a group table for this Galois group.*
Do all the x^2

Problem 151. *Find all subgroups of* $\mathrm{Gal}(\mathbb{Z}_2, GF(8), \iota)$. *"(Hint: there are very few. Use Lagrange's Theorem!)"*

Problem 152. *Compute the Galois Correspondence for* $(\mathbb{Z}_2, GF(8), \iota)$.

Problem 153. *(Optional challenge) Repeat the above exercises for* $GF(16)$. *(That is, first use the Sieve to identify an irreducible quartic in* $\mathbb{Z}_2[x]$, *then use this quartic to construct a field with sixteen elements, then make tables for the Frobenius automorphism and its powers, and finally compute the Galois Correspondence. This is no more conceptually challenging than for* $GF(8)$, *but it is somewhat more tedious. However,* $(\mathbb{Z}_2, GF(16), \iota)$ *is the smallest field extension for which the Galois group has a non-trivial proper subgroup, so it may be of special interest. Though tedious, this example reveals a number of interesting phenomena.)*