MATH 2070A Week 1

Groups

1.1 Overview

- **Groups**
  - How many ways are there to color a cube, such that each face is either black or white?
    Answer: 10. Why?
  - How many ways are there to form a triangle with three sticks of equal lengths, colored red, green and blue, respectively?
  - What are the symmetries of an equilateral triangle?
    Dihedral Group D_3
    IMAGE
- **Rings**
  - Euclidean Algorithm.
  - Chinese Remainder Theorem.
  - Partial Fraction Decomposition.
  - Algebraic Extension of Fields.

1.2 Groups

Definition 1.1. *A group G is a set equipped with a binary operation $* : G \times G \longrightarrow G$ (typically called* **group operation** *or "***multiplication***"), such that:*

- **Associativity**

  $$(a * b) * c = a * (b * c),$$

  for all $a, b, c \in G$. In other words, the group operation is **associative** *.*

- **Existence of an Identity Element**

  There is an element $e \in G$, called an **identity element** *, such that:*

  $$g * e = e * g = g,$$

  for all $g \in G$.

- **Invertibility**

  Each element $g \in G$ has an **inverse** *$g^{-1} \in G$, such that:*

  $$g^{-1} * g = g * g^{-1} = e.$$

- Note that we do not require that $a * b = b * a$.

- We often write ab to denote $a * b$.

Definition 1.2. *If $ab = ba$ for all $a, b \in G$. We say that the group operation is* **commutative***, and that G is an* **abelian group***.*

Example 1.3. *The following sets are groups, with respect to the specified group operations:*

- *$G = \mathbb{Q}\backslash\{0\}$, where the group operation is the usual multiplication for rational numbers. The identity is $e = 1$, and the inverse of $a \in \mathbb{Q}\backslash\{0\}$ is $a^{-1} = \frac{1}{a}$. The group G is abelian.*

- *$G = \mathbb{Q}$, where the group operation is the usual addition $+$ for rational numbers. The identity is $e = 0$. The inverse of $a \in \mathbb{Q}$ with respect to $+$ is $-a$. Note that $\mathbb{Q}$ is NOT a group with respect to multiplication. For in that case, we have $e = 1$, but $0 \in \mathbb{Q}$ has no inverse $0^{-1} \in \mathbb{Q}$ such that $0 \cdot 0^{-1} = 1$.*

Exercise 1.4. *Verify that the following sets are groups under the specified binary operation:*

- $(\mathbb{Z}, +)$
- $(\mathbb{R}, +)$
- $(\mathbb{R}^\times, \cdot)$
- $(U_m, \cdot)$, *where* $m \in \mathbb{N}$,

$$U_m = \{1, \xi_m, \xi_m^2, \ldots, \xi_m^{m-1}\},$$

and $\xi_m = e^{2\pi i/m} = \cos(2\pi/m) + i\sin(2\pi/m) \in \mathbb{C}$.

- *The set of bijective functions* $f : \mathbb{R} \longrightarrow \mathbb{R}$, *where* $f * g := f \circ g$ *(i.e. composition of functions).*

1.2.1 Cayley Table

$*$	a	b	c
a	a^2	ab	ac
b	ba	b^2	bc
c	ca	cb	c^2

Cayley Table for D_3

$*$	r_0	r_1	r_2	s_0	s_1	s_2
r_0	r_0	r_1	r_2	s_0	s_1	s_2
r_1	r_1	r_2	r_0	s_1	s_2	s_0
r_2	r_2	r_0	r_1	s_2	s_0	s_1
s_0	s_0	s_2	s_1	r_0	r_2	r_1
s_1	s_1	s_0	s_2	r_1	r_0	r_2
s_2	s_2	s_1	s_0	r_2	r_1	r_0

1.2.2 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**

5. **WeBWorK**
6. **WeBWorK**
7. **WeBWorK**
8. **WeBWorK**
9. **WeBWorK**

1.2.3 Matrix Groups

Example 1.5. *The set $G = \mathrm{GL}(2, \mathbb{R})$ of real 2×2 matrices with nonzero determinants is a group under matrix multiplication, with identity element:*

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

In the group G, we have:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Note that there are matrices $A, B \in \mathrm{GL}(2, \mathbb{R})$ such that $AB \neq BA$. Hence $\mathrm{GL}(2, \mathbb{R})$ is not abelian.

The group $\mathrm{GL}(2, \mathbb{R})$ is called a **General Linear Group**.

Exercise 1.6. *The set $\mathrm{SL}(2, \mathbb{R})$ of real 2×2 matrices with determinant 1 is a group under matrix multiplication.*

It is called a **Special Linear Group**.

1.2.4 Basic Properties

Claim 1.7. *The identity element e of a group G is unique.*

Proof. Suppose there is an element $e' \in G$ such that $e'g = ge' = g$ for all $g \in G$. Then, in particular, we have:

$$e'e = e$$

But since e is an identity element, we also have $e'e = e'$. Hence, $e' = e$. □

Claim 1.8. *Let G be a group. For all $g \in G$, its inverse g^{-1} is unique.*

Proof. Suppose there exists $g' \in G$ such that $g'g = gg' = e$. By the associativity of the group operation, we have:

$$g' = g'e = g'(gg^{-1}) = (g'g)g^{-1} = eg^{-1} = g^{-1}.$$

Hence, g^{-1} is unique. □

Let G be a group with identity element e. For $g \in G$, $n \in \mathbb{N}$, let:

$$g^n := \underbrace{g \cdot g \cdots g}_{n \text{ times}}.$$
$$g^{-n} := \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}$$
$$g^0 := e.$$

Claim 1.9. *Let G be a group.*

1. *For all $g \in G$, we have:*
$$(g^{-1})^{-1} = g.$$
2. *For all $a, b \in G$, we have:*
$$(ab)^{-1} = b^{-1}a^{-1}.$$
3. *For all $g \in G$, $n, m \in \mathbb{Z}$, we have:*
$$g^n \cdot g^m = g^{n+m}.$$

Proof. **Exercise.** □

Definition 1.10. *Let G be a group, with identity element e. The* **order** *of G is the number of elements in G. The* **order** $\operatorname{ord} g$ *of an $g \in G$ is the smallest $n \in \mathbb{N}$ such that $g^n = e$. If no such n exists, we say that g has* **infinite order**.

Theorem 1.11. *Let G be a group with identity element e. Let g be an element of G. If $g^n = e$ for some $n \in \mathbb{N}$, then $\operatorname{ord} g$ divides n.*

Proof. Shown in class. □

MATH 2070A Week 2

Groups

Definition 2.1. *Let G be a group, with identity element e.*

The **order** *of G is the number of elements in G.*

The **order** $\operatorname{ord} g$ *of an element $g \in G$ is the smallest $n \in \mathbb{N}$ such that $g^n = e$. If no such n exists, we say that g has* **infinite order**.

Theorem 2.2. *Let G be a group with identity element e. Let g be an element of G. If $g^n = e$ for some $n \in \mathbb{N}$, then $\operatorname{ord} g$ is finite, and moreover $\operatorname{ord} g$ divides n.*

Proof. Shown in class. □

Exercise 2.3. *If G has finite order, then every element of G has finite order.*

Definition 2.4. *A group G is* **cyclic** *if there exists $g \in G$ such that every element of G is equal to g^n for some integer n. In which case, we write: $G = \langle g \rangle$, and say that g is a* **generator** *of G.*

Note: The generator of of a cyclic group might not be unique.

Example 2.5. $(U_m, \cdot)$ *is cyclic.*

Exercise 2.6. *A finite cyclic group G has order (i.e. size) n if and only if each of its generators has order n.*

Exercise 2.7. $(\mathbb{Q}, +)$ *is not cyclic.*

2.1 Permutations

Definition 2.8. *Let X be a set. A* **permutation** *of X is a bijective map $\sigma : X \longrightarrow X$.*

Claim 2.9. *The set S_X of permutations of a set X is a group with respect to $\circ$, the composition of maps.*

Proof.

- Let σ, γ be permutations of X. By definition, they are bijective maps from X to itself. It is clear that $\sigma \circ \gamma$ is a bijective map from X to itself, hence $\sigma \circ \gamma$ is a permutation of X. So $\circ$ is a well-defined binary operation on S_X.
- For $\alpha, \beta, \gamma \in S_X$, it is clear that $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$.
- Define a map $e : X \longrightarrow X$ as follows:

  $$e(x) = x, \quad \text{for all } x \in X.$$

  It is clear that $e \in S_X$, and that $e \circ \sigma = \sigma \circ e = \sigma$ for all $\sigma \in S_X$. Hence, e is an identity element in S_X.
- Let σ be any element of S_X. Since $\sigma : X \longrightarrow X$ is by assumption bijective, there exists a bijective map $\sigma^{-1} : X \longrightarrow X$ such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = e$. So σ^{-1} is an inverse of σ with respect to the operation $\circ$.

□

Terminology: We call S_X the **Symmetric Group** on X.
Notation: If $X = \{1, 2, \ldots, n\}$, where $n \in \mathbb{N}$, we denote S_X by S_n.
For $n \in \mathbb{N}$, the group S_n has $n!$ elements.
For $n \in \mathbb{N}$, by definition an element of S_n is a bijective map $\sigma : X \longrightarrow X$, where $X = \{1, 2, \ldots, n\}$. We often describe σ using the following notation:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Example 2.10. *In S_3,*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

is the permutation on $\{1, 2, 3\}$ which sends 1 to 3, 2 to itself, and 3 to 1, i.e. $\sigma(1) = 3, \sigma(2) = 2, \sigma(3) = 1$.
For $\alpha, \beta \in S_3$ given by:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

we have:

$$\alpha\beta = \alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

(since, for example, $\alpha \circ \beta : 1 \overset{\beta}{\mapsto} 2 \overset{\alpha}{\mapsto} 3$*.).*

We also have:

$$\beta\alpha = \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Since $\alpha\beta \neq \beta\alpha$*, the group* S_3 *is non-abelian.*

In general, for $n > 2$*, the group* S_n *is non-abelian (* **Exercise:** *Why?).*

For the same $\alpha \in S_3$ *defined above, we have:*

$$\alpha^2 = \alpha \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

and:

$$\alpha^3 = \alpha \cdot \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

Hence, the order of α *is* 3*.*

2.2 Dihedral Group

Consider the subset $\mathcal{T}$ of transformations of $\mathbb{R}^2$, consisting of all rotations by fixed angles about the origin, and all reflections over lines through the origin.

Consider a regular polygon P with n sides in $\mathbb{R}^2$, centered at the origin. Identify the polygon with its n vertices, which form a subset $P = \{x_1, x_2, \ldots, x_n\}$ of $\mathbb{R}^2$. If $\tau(P) = P$ for some $\tau \in \mathcal{T}$, we say that P is **symmetric** with respect to τ.

Intuitively, it is clear that P is symmetric with respect to n rotations $\{r_0, r_1, \ldots, r_{n-1}\}$, and n reflections $\{s_1, s_2, \ldots, s_n\}$ in $\mathcal{T}$.

IMAGE By Jim.belk - Own work , Public Domain, Link

Theorem 2.11. *The set* $D_n := \{r_0, r_1, \ldots, r_{n-1}, s_1, s_2, \ldots, s_n\}$ *is a group, with respect to the group operation defined by* $\tau * \gamma = \tau \circ \gamma$ *(composition of transformations).*

Terminology: D_n is called a **dihedral group** .

2.3 More on S_n

Consider the following element in S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix}$$

We may describe the action of $\sigma : \{1, 2, \ldots, 6\} \longrightarrow \{1, 2, \ldots, 6\}$ using the notation:

$$\sigma = (15)(246),$$

where $(n_1 n_2 \cdots n_k)$ represents the permutation:

$$n_1 \mapsto n_2 \ldots n_i \mapsto n_{i+1} \cdots \mapsto n_k \mapsto n_1$$

Viewing permutations as bijective maps, the "multiplication" $(15)(246)$ is by definition the composition $(15) \circ (246)$.

We call $(n_1 n_2 \cdots n_k)$ a k**-cycle** . Note that 3 is missing from $(15)(246)$. This corresponds to the fact that 3 is fixed by σ.

Exercise 2.12. *In S_n, for any positive integer $k \leq n$, every k-cycle has order k.*

Claim 2.13. *Every non-identity permutation in S_n is either a cycle or a product of disjoint cycles.*

Proof. Discussed in class. □

Exercise 2.14. *Disjoint cycles commute with each other.*

A 2-cycle is often called a **transposition**, for it switches two elements with each other.

Claim 2.15. *Each element of S_n is a product of (not necessarily disjoint) transpositions.*

Sketch of proof:

Show that each permutation not equal to the identity is a product of cycles, and that each cycle is a product of transpositions:

$$(a_1 a_2 \ldots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2)$$

Example 2.16.

$$\begin{aligned}\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 5 & 4 & 3 & 6 & 1 & 2\end{pmatrix} &= (15)(246)\\ &= (15)(26)(24)\\ &= (15)(46)(26)\end{aligned}$$

Note that a given element σ of S_n may be expressed as a product of transpositions in different ways, but:

Claim 2.17. *In every factorization of σ as a product of transpositions, the number of factors is either always even or always odd.*

Proof. **Exercise.** One approach: Show that there is a unique $n \times n$ matrix, with either 0 or 1 as its coefficients, which sends each standard basis vector $\vec{e}_i$ in $\mathbb{R}^n$ to $\vec{e}_{\sigma(i)}$. Then, use the fact that the determinant of the matrix corresponding to a transposition is -1, and that the determinant function of matrices is multiplicative. □

2.4 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**
5. **WeBWorK**
6. **WeBWorK**

MATH 2070A Week 3

$\mathbb{Z}_n$, Subgroups, Left Cosets, Index

3.1 The Cyclic Group $\mathbb{Z}_n$

Definition 3.1. *Fix an integer $n > 0$.*

For any $k \in \mathbb{Z}$, let $\overline{k}$ denote the remainder of the division of k by n.

Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. We define a binary operation $+_{\mathbb{Z}_n}$ on $\mathbb{Z}_n$ as follows:

$$k +_{\mathbb{Z}_n} l = \overline{k + l}.$$

Exercise 3.2. *$\mathbb{Z}_n = (\mathbb{Z}_n, +_{\mathbb{Z}_n})$ is a* **cyclic** *group, with identity element 0, and $j^{-1} = n - j$ for any nonzero $j \in \mathbb{Z}_n$.*

3.1.1 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**
5. **WeBWorK**
6. **WeBWorK**
7. **WeBWorK**
8. **WeBWorK**
9. **WeBWorK**

10. **WeBWorK**

11. **WeBWorK**

12. **WeBWorK**

3.2 Subgroups

Definition 3.3. *Let G be a group. A subset H of G is a* **subgroup** *of G if it satisfies the following properties:*

- **Closure** *If $a, b \in H$, then $ab \in H$.*
- **Identity** *The identity element of G lies in H.*
- **Inverses** *If $a \in H$, then $a^{-1} \in H$.*

In particular, a subgroup H is a group with respect to the group operation on G, and the identity element of H is the identity element of G.

Example 3.4.

- *For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.*
- *$\mathbb{Q}\backslash\{0\}$ is a subgroup of $(\mathbb{R}\backslash\{0\}, \cdot)$.*
- *$\mathrm{SL}(2, \mathbb{R})$ is a subgroup of $\mathrm{GL}(2, \mathbb{R})$.*
- *The set of all rotations (including the trivial rotation) in a dihedral group D_n is a subgroup of D_n.*
- *Let $n \in \mathbb{N}$, $n \geq 2$. We say that $\sigma \in S_n$ is an* **even permutation** *if it is equal to the product of an even number of transpositions. The subset A_n of S_n consisting of even permutations is a subgroup of S_n. A_n is called an* **alternating group**.

Claim 3.5. *A subset H of a group G is a subgroup of G if and only if H is nonempty and, for all $x, y \in H$, we have $xy^{-1} \in H$.*

Proof. Suppose $H \subseteq G$ is a subgroup. Then, H is nonempty since $e_G \in H$. For all $x, y \in H$, we have $y^{-1} \in H$; hence, $xy^{-1} \in H$.

Conversely, suppose H is a nonempty subset of G, and $xy^{-1} \in H$ for all $x, y \in H$.

- **Identity** Let e be the identity element of G. Since H is nonempty, it contains at least one element h. Since $e = h \cdot h^{-1}$, and by hypothesis $h \cdot h^{-1} \in H$, the set H contains e.

- **Inverses** Since $e \in H$, for all $a \in H$ we have $a^{-1} = e \cdot a^{-1} \in H$.
- **Closure** For all $a, b \in H$, we know that $b^{-1} \in H$. Hence, $ab = a \cdot (b^{-1})^{-1} \in H$.

Hence, H is a subgroup of G. □

Claim 3.6. *The intersection of two subgroups of a group G is a subgroup of G.*

Proof. Exercise. □

Theorem 3.7. *Every subgroup of $(\mathbb{Z}, +)$ is cyclic.*

Proof. Let H be a subgroup of $G = (\mathbb{Z}, +)$. If $H = \{0\}$, then it is clearly cyclic.

Suppose $|H| > 1$. Consider the subset:

$$S = \{h \in H \,:\, h > 0\} \subseteq H$$

Since a subgroup is closed under inverse, and the inverse of any $z \in \mathbb{Z}$ with respect to $+$ is $-z$, the subgroup H must contain at least one positive element. Hence, S is a non-empty subset of $\mathbb{Z}$ bounded from below.

It then follows from the Least Integer Axiom that exists a minimum element h_0 in S. That is $h_0 \leq h$ for any $h \in S$.

Exercise. Show that $H = \langle h_0 \rangle$.

(*Hint* : The Division Theorem for Integers could be useful here.) □

Exercise 3.8. *Every subgroup of a cyclic group is cyclic.*

3.3 Lagrange's Theorem

Let G be a group, H a subgroup of G. We are interested in knowing how large H is relative to G.

We define a relation $\equiv$ on G as follows:

$$a \equiv b \text{ if } b = ah \text{ for some } h \in H,$$

or equivalently:

$$a \equiv b \text{ if } a^{-1}b \in H.$$

Exercise: $\equiv$ is an **equivalence relation**.

We may therefore partition G into disjoint equivalence classes with respect to $\equiv$. We call these equivalence classes the **left cosets** of H.

Each left coset of H has the form $aH = \{ah \,|\, h \in H\}$.

We could likewise define *right* cosets. These sets are of the form Hb, $b \in G$. In general, the number of left cosets and right cosets, if finite, are equal to each other

Example 3.9. *Let $G = (\mathbb{Z}, +)$. Let:*

$$H = 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

The set H is a subgroup of G. The left cosets of H in G are as follows:

$$3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z},$$

where $i + 3\mathbb{Z} := \{i + 3k : k \in \mathbb{Z}\}$.

In general, for $n \in \mathbb{Z}$, the left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are:

$$i + n\mathbb{Z}, \quad i = 0, 1, 2, \ldots, n - 1.$$

Definition 3.10. *The number of left cosets of a subgroup H of G is called the* **index** *of H in G. It is denoted by:*

$$[G : H]$$

Example 3.11. *Let $n \in \mathbb{N}$, $G = (\mathbb{Z}, +)$, $H = (n\mathbb{Z}, +)$. Then,*

$$[G : H] = n.$$

Example 3.12. *Let $G = \mathrm{GL}(2, \mathbb{R})$. Let:*

$$H = \mathrm{GL}^+(2, \mathbb{R}) := \{h \in G : \det h > 0\}.$$

*(***Exercise:** *H is a subgroup of G.)*

Let:

$$s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in G$$

Note that $\det s = \det s^{-1} = -1$.

For any $g \in G$, either $\det g > 0$ *or* $\det g < 0$. *If* $\det g > 0$, *then $g \in H$. If* $\det g < 0$, *we write:*

$$g = (ss^{-1})g = s(s^{-1}g).$$

Since $\det s^{-1}g = (\det s^{-1})(\det g) > 0$, *we have $s^{-1}g \in H$. So, $G = H \sqcup sH$, and $[G : H] = 2$. Notice that both G and H are infinite groups, but the index of H in G is finite.*

Example 3.13. *Let $G = \mathrm{GL}(2, \mathbb{R})$, $H = \mathrm{SL}(2, \mathbb{R})$. For each $x \in \mathbb{R}^\times$, let:*

$$s_x = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \in G$$

Note that $\det s_x = x$.

For each $g \in G$, we have:

$$g = s_{\det g}(s_{\det g}^{-1} g) \in s_{\det g} H$$

Moreover, for distinct $x, y \in \mathbb{R}^\times$, we have:

$$\det(s_x^{-1} s_y) = y/x \neq 1.$$

This implies that $s_x^{-1} s_y \notin H$, hence $s_y H$ and $s_x H$ are disjoint cosets. We have therefore:

$$G = \bigsqcup_{x \in \mathbb{R}^\times} s_x H.$$

The index $[G : H]$ in this case is infinite.

MATH 2070A Week 4

Lagrange's Theorem, Generators, Group Homomorphisms

4.1 Lagrange's Theorem

Theorem 4.1 (Lagrange's Theorem)**.** *Let G be a finite group. Let H be subgroup of G, then $|H|$ divides $|G|$. More precisely, $|G| = [G : H] \cdot |H|$.*

Proof. We already know that the left cosets of H partition G. That is:

$$G = a_1 H \sqcup a_2 H \sqcup \ldots \sqcup a_{[G:H]} H,$$

where $a_i H \cap a_j H = \emptyset$ if $i \neq j$. Hence, $|G| = \sum_{i=1}^{[G:H]} |a_i H|$.

The theorem follows if we show that the size of each left coset of H is equal to $|H|$.

For each left coset S of H, pick an element $a \in S$, and define a map $\psi : H \longrightarrow S$ as follows:

$$\psi(h) = ah.$$

We want to show that ψ is bijective.

For any $s \in S$, by definition of a left coset (as an equivalence class) we have $s = ah$ for some $h \in H$. Hence, ψ is surjective.

If $\psi(h') = ah' = ah = \psi(h)$ for some $h', h \in H$, then $h' = a^{-1}ah' = a^{-1}ah = h$. Hence, ψ is one-to-one.

So we have a bijection between two finite sets. Hence, $|S| = |H|$. □

Corollary 4.2. *Let G be a finite group. The order of every element of G divides the order of G.*

Since G is finite, any element of $g \in G$ has finite order $\operatorname{ord} g$. Since the order of the subgroup:

$$H = \langle g \rangle = \{e, g, g^2, \ldots, g^{(\operatorname{ord} g)-1}\}$$

is equal to $\operatorname{ord} g$, it follows from Lagrange's Theorem that $\operatorname{ord} g = |H|$ divides $|G|$.

Corollary 4.3. *If the order of a group G is prime, then G is a cyclic group. @refpf:primecyclic*

Corollary 4.4. *If a group G is finite, then for all $g \in G$ we have:*

$$g^{|G|} = e.$$

@refpf:ghatordGeqe

Corollary 4.5. *Let G be a finite group. Then a nonempty subset H of G is a subgroup of G if and only if it is closed under the group operation of G (i.e. $ab \in H$ for all $a, b \in H$).*

Proof. It is easy to see that if H is a subgroup, then it is closed under the group operation. The other direction is left as an **Exercise** . □

Example 4.6. *Let n be an integer greater than 1. The group A_n of even permutations on a set of n elements (see Example 3.4) has order $\frac{n!}{2}$.*

Proof. View A_n as a subgroup of S_n, which has order $n!$.
Exercise : Show that $S_n = A_n \sqcup (12)A_n$.
Hence, we have $[S_n : A_n] = 2$.
It now follows from Lagrange's Theorem that:

$$|A_n| = \frac{|S_n|}{[S_n : A_n]} = \frac{n!}{2}.$$

□

4.1.1 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**

4.2 Generators

Let G be a group, X a nonempty subset of G. The subset of G consisting of elements of the form:

$$g_1^{m_1} g_2^{m_2} \cdots g_n^{m_n}, \quad \text{where} \quad n \in \mathbb{N}, g_i \in X, m_i \in \mathbb{Z},$$

is a subgroup of G. We say that it is the subgroup of G **generated** by X. If $X = \{x_1, x_2, \ldots, x_l\}$, $l \in \mathbb{N}$. We often write:

$$\langle x_1, x_2, \ldots, x_l \rangle$$

to denote the subgroup generated by X.

Example 4.7. *In D_n, $\{r_0, r_1, \ldots, r_{n-1}\} = \langle r_1 \rangle$.*

If there exists a finite number of elements $x_1, x_2, \ldots, x_l \in G$ such that $G = \langle x_1, x_2, \ldots, x_l \rangle$, we say that G is **finitely generated** .

For example, every cyclic group is finitely generated, for it is generated by one element.

Every finite group is finitely generated, since we may take the finite generating set X to be G itself.

Example 4.8. *Consider $G = D_3$, and its subgroup $H = \{r_0, r_1, r_2\}$ consisting of its rotations. (We use the convention that r_k is the anticlockwise rotation by an angle of $2\pi k/3$).*

By Lagrange's Theorem, the index of H in G is $[G : H] = |G| / |H| = 2$. This implies that $G = H \sqcup gH$ for some $g \in G$. Since $gH = H$ if $g \in H$, we may conclude that $g \notin H$. So, g is a reflection.

Conversely, for any reflection $s \in D_3$, the left coset sH is disjoint from H. We have therefore $G = H \sqcup s_1 H = H \sqcup s_2 H = H \sqcup s_3 H$, which implies that $s_1 H = s_2 H = s_3 H$.

In particular, for a fixed $s = s_i$, any element in G is either a rotation or equal to sr_i for some rotation r_i. Since H is a cyclic group, generated by the rotation r_1, we have $D_3 = \langle r_1, s \rangle$, where s is any reflection in D_3.

4.3 Group Homomorphisms

Definition 4.9. *Let $G = (G, *)$, $G' = (G', *')$ be groups. A* **group homomorphism** *ϕ from G to G' is a map $\phi : G \longrightarrow G'$ which satisfies:*

$$\phi(a * b) = \phi(a) *' \phi(b),$$

for all $a, b \in G$.

Claim 4.10. *If $\phi : G \longrightarrow G'$ is a group homomorphism, then:*

1. $\phi(e_G) = e_{G'}$.
2. $\phi(g^{-1}) = \phi(g)^{-1}$, *for all* $g \in G$.
3. $\phi(g^n) = \phi(g)^n$, *for all* $g \in G$, $n \in \mathbb{Z}$.

Proof. We prove the first claim, and leave the rest as an exercise. Since e_G is the identity element of G, we have $e_G * e_G = e_G$. On the other hand, since ϕ is a group homomorphism, we have:

$$\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) *' \phi(e_G).$$

Since G' is a group, $\phi(e_G)^{-1}$ exists in G', hence:

$$\phi(e_G)^{-1} *' \phi(e_G) = \phi(e_G)^{-1} *' (\phi(e_G) *' \phi(e_G))$$

The left-hand side is equal to $e_{G'}$, while by the associativity of $*'$ the right-hand side is equal to $\phi(e_G)$. □

Let $\phi : G \longrightarrow G'$ be a homomorphism of groups. The image of ϕ is defined as:

$$\operatorname{im} \phi := \phi(G) := \{g' \in G' : g' = \phi(g) \text{ for some } g \in G\} \subseteq G'$$

The kernel of ϕ is defined as:

$$\ker \phi = \{g \in G : \phi(g) = e_{G'}\} \subseteq G.$$

Claim 4.11. *The image of ϕ is a subgroup of G'. The kernel of ϕ is a subgroup of G.*

Claim 4.12. *A group homomorphism $\phi : G \longrightarrow G'$ is one-to-one if and only if* $\ker \phi = \{e_G\}$. *@refpf:kernelonetoone*

Example 4.13 (Examples of Group Homomorphisms)**.**

- $\phi : S_n \longrightarrow (\{\pm 1\}, \cdot)$,

$$\phi(\sigma) = \begin{cases} 1, & \sigma \text{ is an even permutation.} \\ -1, & \sigma \text{ is an odd permutation.} \end{cases}$$

  $\ker \phi = A_n$.

- $\det : \mathrm{GL}(n, \mathbb{R}) \longrightarrow (\mathbb{R}^\times, \cdot)$

  $\ker \det = \mathrm{SL}(n, \mathbb{R})$.

- *Let G be the (additive) group of all real-valued continuous functions on $[0,1]$.*

$$\phi : G \longrightarrow (\mathbb{R}, +)$$
$$\phi(f) = \int_0^1 f(x)\,dx.$$

- $\phi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^\times, \cdot)$.

$$\phi(x) = e^x.$$

Definition 4.14. *Let G, G' be groups. A map $\phi : G \longrightarrow G'$ is a group* **isomorphism** *if it is a bijective group homomorphism.*

Note that if a homomorphism ϕ is bijective, then $\phi^{-1} : G' \longrightarrow G$ is also a homomorphism, and consequently, ϕ^{-1} is an isomorphism. If there exists an isomorphism between two groups G and G', we say that the groups G and G' are **isomorphic** .

Example 4.15. *Recall Definition 3.1 and Exercise 3.2.*

Let $n > 2$. Let $H = \{r_0, r_1, r_2, \ldots, r_{n-1}\}$ be the subgroup of D_n consisting of all rotations, where r_1 denotes the anticlockwise rotation by the angle $2\pi/n$, and $r_k = r_1^k$. Then, H is isomorphic to $\mathbb{Z}_n = (\mathbb{Z}_n, +_{\mathbb{Z}_n})$.

Proof. Define $\phi : H \longrightarrow \mathbb{Z}_n$ as follows:

$$\phi(r_k) = k, \quad k \in \{0, 1, 2, \ldots, n-1\}.$$

For any $k \in \mathbb{Z}$, let $\overline{k} \in \{0, 1, 2, \ldots, n-1\}$ denote the remainder of the division of k by n. By the Division Theorem for Integers, we have:

$$k = nq + \overline{k}$$

for some integer $q \in \mathbb{Z}$.

It now follows from $\operatorname{ord} r_1 = n$ that, for all $r_i, r_j \in H$, we have:

$$\begin{aligned} r_i r_j &= r_1^i r_1^j = r_1^{i+j} \\ &= r_1^{nq+\overline{i+j}} \\ &= (r_1^n)^q\, r_1^{\overline{i+j}} \\ &= r_{\overline{i+j}}. \end{aligned}$$

Hence,

$$\begin{aligned} \phi(r_i r_j) &= \phi(r_{\overline{i+j}}) \\ &= \overline{i+j} \\ &= i +_{\mathbb{Z}_n} j \\ &= \phi(r_i) +_{\mathbb{Z}_n} \phi(r_j). \end{aligned}$$

This shows that ϕ is a homomorphism. It is clear that ϕ is surjective, which then implies that ϕ is one-to-one, for the two groups have the same size. Hence, ϕ is a bijective homomorphism, i.e. an isomorphism. $\square$

MATH 2070A Week 5

Group Homomorphisms, Rings

Claim 5.1. *Any cyclic group of finite order n is isomorphic to $\mathbb{Z}_n$.*

Proof. Sketch of Proof:

By definition, a cyclic group G is equal to $\langle g \rangle$ for some $g \in G$. Moreover, $\operatorname{ord} g = \operatorname{ord} G$.

Define a map $\phi : G \longrightarrow \mathbb{Z}_n$ as follows:

$$\phi(g^k) = k, \quad k \in \{0, 1, 2, \ldots, n-1\}.$$

Show that ϕ is a group isomorphism.

(For reference, see the discussion of Example 4.15.) □

Corollary 5.2. *If G and G' are two finite cyclic groups of the same order, then G is isomorphic to G'.*

Exercise 5.3. *An infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.*

Exercise 5.4. *Let G be a cyclic group, then any group which is isomorphic to G is also cyclic.*

5.1 Product Group

Let $(A, *_A), (B, *_B)$ be groups. The direct product:

$$A \times B := \{(a, b) \mid a \in A, b \in B\}$$

has a natural group structure where the group operation $*$ is defined as follows:

$$(a, b) * (a', b') = (a *_A a', b *_B b'), \quad (a, b), (a', b') \in A \times B.$$

The identity element of $A \times B$ is $e = (e_A, e_B)$, where e_A, e_B are the identity elements of A and B, respectively.

For any $(a, b) \in A \times B$, we have $(a, b)^{-1} = (a^{-1}, b^{-1})$, where a^{-1}, b^{-1} are the inverses of a, b in the groups A, B, respectively.

For any collection of groups $A_1, A_2, \ldots, A_n$, we may similarly define a group operation $*$ on:

$$A_1 \times A_2 \times \cdots \times A_n := \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i, i = 1, 2, \ldots n\}.$$

That is:

$$(a_1, a_2, \ldots, a_n) * (a_1', a_2', \ldots, a_n') = (a_1 *_{A_1} a_1', a_2 *_{A_2} a_2', \ldots, a_n *_{A_n} a_n')$$

The identity element of $A_1 \times A_2 \times \cdots \times A_n$ is:

$$e = (e_{A_1}, e_{A_2}, \ldots, e_{A_n}).$$

For any $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$, its inverse is:

$$(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}).$$

Exercise 5.5. *$\mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$.*

Proof. **Hint:**
Show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group generated by $(1, 1)$. □

Example 5.6. *The cyclic group $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. Each element of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ is of order at most 2. Since $|G| = 4$, G cannot be generated by a single element. Hence, G is not cyclic, so it cannot be isomorphic to the cyclic group $\mathbb{Z}_4$. □

Exercise 5.7. *Let G be an abelian group, then any group which is isomorphic to G is abelian.*

Example 5.8. *The group D_6 has 12 elements. We have seen that $D_6 = \langle r_1, s \rangle$, where r_1 is a rotation of order 6, and s is a reflection, which has order 2. So, it is reasonable to ask if D_6 is isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_2$. The answer is no. For $\mathbb{Z}_6 \times \mathbb{Z}_2$ is abelian, but D_6 is not.*

Claim 5.9. *The dihedral group D_3 is isomorphic to the symmetric group S_3.*

Proof. We have seen that $D_3 = \langle r, s \rangle$, where $r = r_1$ and s is any fixed reflection, with:

$$\operatorname{ord} r = 3, \quad \operatorname{ord} s = 2, \quad srs = r^{-1}.$$

In particular , any element in D_3 may be expressed as $r^i s^j$, with $i \in \{0,1,2\}$, $j \in \{0,1\}$.

We have also seen that $S_3 = \langle a, b \rangle$, where:

$$a = (123), \quad b = (12), \quad \operatorname{ord} a = 3, \quad \operatorname{ord} b = 2, \quad bab = a^{-1}.$$

Hence, any element in S_3 may be expressed as $a^i b^j$, with $i \in \{0,1,2\}$, $j \in \{0,1\}$.

Define map $\phi : D_3 \longrightarrow S_3$ as follows:

$$\phi(r^i s^j) = a^i b^j, \quad i, j \in \mathbb{Z}$$

We first show that ϕ is well-defined: That is, whenever $r^i s^j = r^{i'} s^{j'}$, we want to show that:

$$\phi(r^i s^j) = \phi(r^{i'} s^{j'}).$$

The condition $r^i s^j = r^{i'} s^{j'}$ implies that:

$$r^{i-i'} = s^{j'-j}$$

This holds only if $r^{i-i'} = s^{j'-j} = e$, since no rotation is a reflection.

Since $\operatorname{ord} r = 3$ and $\operatorname{ord} s = 2$, we have:

$$3|(i - i'), \quad 2|(j' - j),$$

by Theorem 2.2.

Hence,

$$\begin{aligned}
\phi(r^i s^j)\phi(r^{i'} s^{j'})^{-1} &= (a^i b^j)(a^{i'} b^{j'})^{-1} \\
&= a^i b^j b^{-j'} a^{-i'} \\
&= a^i b^{j-j'} a^{-i'} \\
&= a^{i-i'} && \text{since } \operatorname{ord} b = 2. \\
&= e && \text{since } \operatorname{ord} a = 3.
\end{aligned}$$

This implies that $\phi(r^i s^j) = \phi(r^{i'} s^{j'})$. We conclude that ϕ is well-defined.

We now show that ϕ is a group homomorphism:

Given $\mu, \mu' \in \{0,1,2\}$, $\nu, \nu' \in \{0,1\}$, we have:

$$\phi(r^\mu s^\nu \cdot r^{\mu'} s^{\nu'}) = \begin{cases} \phi(r^{\mu+\mu'} s^{\nu'}), & \text{if } \nu = 0; \\ \phi(r^{\mu-\mu'} s^{\nu+\nu'}), & \text{if } \nu = 1. \end{cases}$$

$$= \begin{cases} a^{\mu+\mu'} b^{\nu'}, & \text{if } \nu = 0; \\ a^{\mu-\mu'} b^{\nu+\nu'} = a^\mu b^\nu a^{\mu'} b^{\nu'}, & \text{if } \nu = 1. \end{cases}$$

$$= \phi(r^\mu s^\nu)\phi(r^{\mu'} s^{\nu'}).$$

This shows that ϕ is a group homomorphism.

To show that ϕ is a group isomorphism, it remains to show that it is surjective and one-to-one.

It is clear that ϕ is surjective. We leave it as an exercise to show that ϕ is one-to-one. □

Example 5.10. *The group:*

$$G = \left\{ g \in \mathrm{GL}(2,\mathbb{R}) \;\middle|\; g = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ for some } \theta \in \mathbb{R} \right\}$$

is isomorphic to

$$G' = \{z \in \mathbb{C} : |z| = 1\}.$$

Here, the group operation on G is matrix multiplication, and the group operation on G' is the multiplication of complex numbers.

Each element in G' is equal to $e^{i\theta}$ for some $\theta \in \mathbb{R}$. Define a map $\phi : G \longrightarrow G'$ as follows:

$$\phi\left(\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\right) = e^{i\theta}.$$

Exercise: *Show that ϕ is a well-defined map. Then, show that it is a bijective group homomorphism.*

5.1.1 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**
5. **WeBWorK**
6. **WeBWorK**

5.2 Rings

5.2.1 Basic Results in Elementary Number Theory

Theorem 5.11 (Division Theorem)**.** *Let $a, b \in \mathbb{Z}$, $a \neq 0$, then there exist unique q (called the quotient), and r (***remainder***) in $\mathbb{Z}$, satisfying $0 \leq r < |a|$, such that $b = aq + r$.*

Proof. We will prove the case $a > 0$, $b \geq 0$. The other cases are left as exercises.

Fix $a > 0$. First, we prove the existence of the quotient q and remainder r for any $b \geq 0$, using mathematical induction.

The base step corresponds to the case $0 \leq b < a$. In this case, if we let $q = 0$ and $r = b$, then indeed $b = qa + r$, where $0 \leq r = b < a$. Hence, q and r exist.

The inductive step of the proof of the existence of q and r is as follows: Suppose the existence of the quotient and remainder holds for all non-negative $b' < b$, we want to show that it must also hold for b.

First, we may assume that $b \geq a$, since the case $b < a$ has already been proved. Let $b' = b - a$. Then, $0 \leq b' < b$, so by the inductive hypothesis we have $b' = q'a + r'$ for some $q', r' \in \mathbb{Z}$ such that $0 \leq r' < a$.

This implies that $b = b' + a = (q' + 1)a + r'$.

So, if we let $q = q' + 1$ and $r = r'$, then $b = qa + r$, where $0 \leq r < a$. This establishes the existence of q, r for b. Hence, by mathematical induction, the existence of q, r holds for all $b \geq 0$.

Now we prove the uniqueness of q and r. Suppose $b = qa + r = q'a + r'$, where $q, q', r, r' \in \mathbb{Z}$, with $0 \leq r, r' < a$.

Then, $qa + r = q'a + r'$ implies that $r - r' = (q' - q)a$. Since $0 \leq r, r' < a$, we have:

$$a > |r - r'| = |q' - q|\, a.$$

Since $q' - q$ is an integer, the above inequality implies that $q' - q = 0$, i.e. $q' = q$, which then also implies that $r' = r$. We have therefore established the uniqueness of q and r.

The proof of the theorem, for the case $a > 0, b \geq 0$, is now complete. □

Another Proof of the Division Theorem.

Proof. We consider here the special case $b \geq 0$. Consider the set:

$$S = \{s \in \mathbb{Z}_{\geq 0} \ : \ s = b - aq \text{ for some } q \in \mathbb{Z}.\}$$

Since $b = b - a \cdot 0 \geq 0$, we have $b \in S$. So, S is a nonempty subset of $\mathbb{Z}$ bounded below by 0. By the Least Integer Axiom, there exists a minimum element $r \in S$. We claim that $r < |a|$:

Suppose not, that is, $r \geq |a|$. By assumption: $r = b - aq$ for some $q \in \mathbb{Z}$.

Consider the element $r' = r - |a|$. Then, $0 \leq r'$ and moreover:

$$r' = (b - aq) - |a| = b - (q \pm 1)a,$$

depending on whether $a > 0$ or $a < 0$. So, $r' \in S$. On the other hand, by construction we have $r' < r$, which contradicts the minimality of r. We conclude that $r < |a|$. This establishes the existence of the remainder r.

The existence of q in the theorem is now also clear. We leave the proof of the uniqueness of r and q as an exercise. □

Theorem 5.12. *Every subgroup of $\mathbb{Z}$ is cyclic.*

Proof. First, we note that the group operation $*$ on $\mathbb{Z}$ is integer addition, with $e_{\mathbb{Z}} = 0$, and $z^{*-1} = -z$ for any $z \in \mathbb{Z}$.

Let H be a nontrivial (i.e. contains more than one element) subgroup of $\mathbb{Z}$. Since for any $h \in H$ we also have $-h \in H$, H contains at least one positive element.

Let d be the least positive integer in H. It exists because of the Least Integer Axiom.

We claim that $H = \langle d \rangle$:

For any $h \in H$, by the Division Theorem for Integers we have $h = dq + r$ for some $r, q \in \mathbb{Z}$, such that $0 \leq r < d$. Then,

$$r = h - dq = h - (\underbrace{d + d + \ldots + d}_{q \text{ times}})$$

if $q \geq 0$, or

$$r = h - dq = h - (\underbrace{(-d) + (-d) + \ldots + (-d)}_{q \text{ times}})$$

if $q < 0$.

In either case, since H is a subgroup we have $r \in H$. If $r > 0$, then we have a positive element in H which is strictly less than d, which contradicts the minimality of d. Hence, $r = 0$, from which it follows that any $h \in H$ is equal to $dq = d^{*q}$ for some $q \in \mathbb{Z}$. This shows that $H = \langle d \rangle$. □

Exercise 5.13. *Let n be a positive integer. Every subgroup of $\mathbb{Z}_n$ is cyclic.*

Corollary 5.14. *Every subgroup of a cyclic group is cyclic.*

MATH 2070A Week 6

Elementary Number Theory, Euclid's Lemma, Congruences, Chinese Remainder Theorem

---

6.1 Further Results in Elementary Number Theory

Definition 6.1. *The* **Greatest Common Divisor** $gcd(a, b)$ *of* $a, b \in \mathbb{Z}$ *is the largest positive integer* d *which divides both* a *and* b *(Notation:* $d|a$ *and* $d|b$*).*

Note. If $a \neq 0$, then $gcd(a, 0) = |a|$. $gcd(0, 0)$ is undefined.

6.1.1 Euclidean Algorithm

Lemma 6.2. *If* $b = aq + r$ $(a, b, q, r \in \mathbb{Z})$*, then* $gcd(b, a) = gcd(a, r)$.

Proof. If $d|a$ and $d|b$, then $d|r = b - aq$. Conversely, if $d|a$ and $d|r$, then $d|a$ and $d|b = qa + r$. So, the set of common divisors of a, b is the same as the set of the common divisors of a, r. If two finite sets of integers are the same, then their largest elements are clearly the same. In other words:

$$gcd(b, a) = gcd(a, r).$$

□

Suppose $|b| \geq |a|$. Let $b_0 = b$, $a_0 = a$. Write $b_0 = a_0 q_0 + r_0$, where $0 \leq r_0 < |a_0|$.

For $n > 0$, let $b_n = a_{n-1}$ and $a_n = r_{n-1}$, where r_n is the remainder of the division of b_n by a_n. That is,

$$b_n = a_n q_n + r_n, \quad 0 \leq r_n < |a_n|.$$

If $r_0 = 0$, then that means that $a|b$, and $gcd(a, b) = |a|$. Now, suppose $r_0 > 0$. Since r_n is a non-negative integer and $0 \leq r_n < r_{n-1}$, eventually, $r_n = 0$ for some $n \in \mathbb{N}$.

Claim 6.3. $gcd(b, a) = |a_n|$.

Proof. By the previous lemma,

$$\begin{aligned} gcd(b, a) &= gcd(b_0, a_0) \\ &= gcd(a_0, r_0) = gcd(b_1, a_1) \\ &= gcd(a_1, r_1) = gcd(b_2, a_2) \\ &= \dots \\ &= gcd(a_n, r_n) = gcd(a_n, 0) = |a_n| . \end{aligned}$$

□

Example 6.4. *Find* $gcd(285, 255)$.

$$\begin{aligned} \underbrace{285}_{b_0} &= \underbrace{255}_{a_0}\underbrace{1}_{q_0} + \underbrace{30}_{r_0} \\ \underbrace{255}_{b_1=a_0} &= \underbrace{30}_{a_1=r_0}\underbrace{8}_{q_1} + \underbrace{15}_{r_1} \\ \underbrace{30}_{b_2} &= \underbrace{15}_{a_2}\underbrace{2}_{q_2} + \underbrace{0}_{r_2} \end{aligned}$$

So, $gcd(285, 255) = r_1 = 15$.

Claim 6.5 (Bézout's Lemma)**.** *Let* a, b *be nonzero integers. There exist* $x, y \in \mathbb{Z}$ *such that* $gcd(a, b) = ax + by$.

Proof. **Sketch of Proof:**

Approach 1. Recall the notation used in Section 6.1.1 () . We saw that if $r_n = 0$, then $gcd(a, b) = r_{n-1}$.

We may prove Bézout's Lemma via mathematical induction as follows:

First, for integers $0 \leq l < \min(n - 1, 2)$, show that there exist $x_l, y_l \in \mathbb{Z}$ such that $r_l = ax_l + by_l$. This is the base step of the induction proof.

We now carry out the inductive step. Suppose $n - 1 \geq 2$. For any integer $2 \leq k \leq n - 1$, suppose $r_l = ax_l + by_l$ for some $x_l, y_l \in \mathbb{Z}$, for all $0 \leq l < k$.

Show that:

$$r_k = \underbrace{b_k}_{a_{k-1}=r_{k-2}} - q_k \underbrace{a_k}_{r_{k-1}}$$

also has the form $r_k = ax_k + by_k$ for some $x_k, y_k \in \mathbb{Z}$.

The desired identity $gcd(a, b) = r_{n-1} = ax_{n-1} + by_{n-1}$ then follows by mathemtical induction.

Approach 2. Consider the set:

$$S = \{n \in \mathbb{Z}_{>0} | n = ax + by \text{ for some } x, y \in \mathbb{Z}\}.$$

Show that the the minimum element $d \in S$ is the greatest common divisor of a and b.

□

Exercise 6.6. *Find $x, y \in \mathbb{Z}$ such that:*

$$gcd(285, 255) = 285x + 255y.$$

Exercise 6.7. *For any nonzero a, b in the group $G = (\mathbb{Z}, +)$, we have:*

$$\langle a, b \rangle = \langle gcd(a, b) \rangle.$$

Definition 6.8. *Two integers $a, b \in \mathbb{Z}$ are* **relatively prime** *if $gcd(a, b) = 1$.*

Claim 6.9. *Two integers $a, b \in \mathbb{Z}$ are relatively prime if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*

Proof. If a, b are relatively prime, then by definition $gcd(a, b) = 1$. So, by Bézout's Lemma there exist $x, y \in \mathbb{Z}$ such that:

$$ax + by = gcd(a, b) = 1.$$

Conversely, suppose $ax + by = 1$ for some $x, y \in \mathbb{Z}$. Then, any common divisor of a and b must also be a divisor of 1. Since 1 is only divisible by ± 1, we conclude that $gcd(a, b) = 1$. □

Definition 6.10. *An integer $p \geq 2$ is* **prime** *if its only proper divisors (i.e. divisors different from $\pm p$) are ± 1.*

Lemma 6.11 (Euclid's Lemma)**.** *Let a, b be integers. If p is prime and $p|ab$, then p divides at least one of a and b.*

Proof. Suppose p does not divide b (Notation: $p \nmid b$), then $gcd(p, b) = 1$, which implies that $1 = px + by$ for some $x, y \in \mathbb{Z}$. Since $p|apx$ and $p|aby$, we have $p|a = a\underbrace{(px + by)}_{=1}$. □

More generally,

Claim 6.12. *If a, b are relatively prime and $a|bc$, then $a|c$.*

Proof. **Exercise.** □

Claim 6.13. *If a, b are relatively prime and:*

$$a|c, \quad b|c,$$

then:

$$ab|c.$$

Proof. By assumption, there are $s, t \in \mathbb{Z}$ such that:

$$c = as = bt.$$

So, $a|as = bt$, which by Claim 6.12 implies that $a|t$, since $gcd(a, b) = 1$.

Hence, $t = au$ for some $u \in \mathbb{Z}$, and we have $c = bt = abu$. It follows that $ab|c$. □

Theorem 6.14 (The Fundamental Theorem of Arithmetic)**.** *Let a be a positive integer ≥ 2. Then,*

1. *The integer a is either a prime or a product of primes.*
2. **Unique Factorization** *The integer a may be written uniquely as*

$$a = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l},$$

where $p_1, p_2, \cdots, p_l$ are distinct prime numbers, and $n_1, n_2, \ldots, n_l \in \mathbb{N}$.

Proof. We prove Part 1 of the theorem by contradiction.

Suppose there exist positive integers ≥ 2 which are neither primes nor products of primes.

Let m be the smallest such integer. Since m is not prime, there are positive integers $a, b \neq 1$ such that $m = ab$.

In particular, $a, b < m$. So, a and b must be either primes or products of primes, which implies that m is itself a product of primes, a contradiction.

We now prove Part 2 (**Unique Factorization**) of the theorem by induction.

The base step corresponds to the case $l = 1$.

Suppose:

$$a = p_1^{n_1} = q_1^{m_1} q_2^{m_2} \cdots q_k^{m_k},$$

where p_1 is prime, and the q_i's are distinct primes, and $n_1, m_i \in \mathbb{N}$.

Then, p_1 divides the right-hand side, so by Euclid's Lemma p_1 divides one of the q_i's.

Since the q_i's are prime, we may assume (reindexing if necessary) that $p_1 = q_1$.

Suppose $k > 1$. If $n_1 > m_1$, then $p_1^{n_1 - m_1} = q_2^{m_2} \cdots q_k^{m_k}$, which implies that $p_1 = q_1$ is one of $q_2, \ldots, q_k$, a contradiction, since the q_i's are distinct.

If $n_1 \leq m_1$, then $1 = p_1^{m_1 - n_1} q_2^{m_2} \cdots q_k^{m_k}$, which is impossible. We conclude that $k = 1$, and $p_1 = q_1$, $n_1 = m_1$.

Now we establish the inductive step: Suppose unique factorization is true for all positive integers a' which may be written as $a' = p_1^{n_1} p_2^{n_2} \cdots p_{l'}^{n_{l'}}$, for any $l' < l$. We want to show that it is also true for any integer a which may be written as $a = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l}$.

In other words, suppose

$$a = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l} = q_1^{m_1} \cdots q_k^{m_k},$$

where p_i, q_i are prime and $n_i, m_i \in \mathbb{N}$. We want to show that $k = l$, and $p_i = q_i$, $n_i = m_i$, for $i = 1, 2, \ldots, l$.

If $k < l$, then by the inductive hypothesis applied to $l' = k < l$, we have $k = l$, a contradiction. So, we may assume that $k \geq l$.

By Euclid's Lemma, p_l divides, and hence must be equal to, one of the q_i's.

Reindexing if necessary, we may assume that $p_l = q_k$. Cancelling p_l and q_k from both sides of the equation, it is also clear that $n_l = m_k$. Hence, we have:

$$p_1^{n_1} p_2^{n_2} \cdots p_{l-1}^{n_{l-1}} = q_1^{m_1} \cdots q_{k-1}^{m_{k-1}}.$$

Since $l - 1 < l$, we may now apply the inductive hypothesis to the integer which is equal to the left-hand side of the above equation, and conclude that $l - 1 = k - 1$, $p_i = q_i$, $n_i = m_i$, for $1 \leq i \leq l - 1$.

Since we already know that $p_l^{n_l}$ matches $q_k^{m_k}$, we have $l = k$, and $p_i = q_i$, $n_i = m_i$, for $1 \leq i \leq l$. This establishes the inductive step, and completes the proof. □

6.1.2 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**

6.2 Modular Arithmetic

Definition 6.15. *Let m be a positive integer, then $a, b \in \mathbb{Z}$ are said to be:*
congruent modulo m

$$a \equiv b \mod m,$$

if $m|(a-b)$.

Claim 6.16. *The congruence relation $\equiv$ is an* **equivalence relation** *. In other words, it is:*

- **Reflexive***:*
  $a \equiv a \mod m$*;*
- **Symmetric***:*
  $a \equiv b \mod m$ *implies that* $b \equiv a \mod m$*;*
- **Transitive***:*
  $a \equiv b \mod m$*,* $b \equiv c \mod m$*, imply that* $a \equiv c \mod m$*.*

Proof.
- **Reflexivity** Since $m|0 = (a-a)$, we have $a \equiv a \mod m$.
- **Symmetry** If $a \equiv b \mod m$, then by definition m divides $a-b$. But if m divides $a-b$, it must also divide $-(a-b) = b-a$, which implies that $b \equiv a \mod m$.
- **Transitivity** If $m|(a-b)$ and $m|(b-c)$, then $m|((a-b)+(b-c)) = (a-c)$, which implies that $a \equiv c \mod m$.

□

Note. $a \equiv 0 \mod m$ if and only if $m|a$.

Claim 6.17. *1. If $a = qm + r$, then $a \equiv r \mod m$.*

2. If $0 \leq r < r' < m$, then $r \not\equiv r' \mod m$.

Proof. **Exercise.** □

Corollary 6.18. *Given integer $m \geq 2$, every $a \in \mathbb{Z}$ is congruent modulo m to exactly one of $\{0, 1, 2, \ldots, m-1\}$.*

Proof. By Part 1 of the claim, a is congruent mod m to the remainder r of the division of a by m.

By definition, the remainder r lies in $\{0, 1, 2, \ldots, m-1\}$. If $a \equiv r' \mod m$, for some $r' \in \{0, 1, 2, \ldots, m-1\}$, then by transitivity, we have $r' \equiv r \mod m$.

By Part 2 of the claim, we have $r = r'$. □

Theorem 6.19. *Congruence is compatible with addition and multiplication in the following sense:*

- **Addition** *If* $a \equiv a' \mod m$*, and* $b \equiv b' \mod m$*, then* $a + b \equiv a' + b' \mod m$*.*
- **Multiplication** *If* $a \equiv a' \mod m$ *and* $b \equiv b' \mod m$*, then* $ab \equiv a'b' \mod m$*.*

Proof.

- **Addition** If $m|(a - a')$ and $m|(b - b')$, then:

$$m|(a - a') + (b - b') = (a + b) - (a' + b').$$

So, $a + b \equiv a' + b' \mod m$.

- **Multiplication** If $m|(a - a')$ and $m|(b - b')$, then:

$$m|(a - a')b + a'(b - b') = (ab - a'b').$$

So, $ab \equiv a'b' \mod m$.

□

Example 6.20. *For* $a \in \mathbb{Z}$*,* $a^2 \equiv 0, 1,$ *or* $4 \mod 8$*.*

Proof. By Corollary 6.18 , any $a \in \mathbb{Z}$ is congruent modulo 8 to exactly one element in $\{0, 1, 2, \ldots, 7\}$. So, by Theorem 6.19 , a^2 is congruent modulo 8 to one of:

$$\{0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2\} = \{0, 1, 4, 9, 16, 25, 36, 49\}.$$

The numbers above a congruent modulo 8 to 0, 1, or 4. The claim follows. □

Theorem 6.21. *If* a *and* m *are relatively prime, then there exists* $x \in \mathbb{Z}$ *such that* $ax \equiv 1 \mod m$*.*

Proof. Since a and m are relatively prime, by Bézout's Lemma there exist $x, y \in \mathbb{Z}$ such that:

$$ax + my = 1.$$

This implies that m divides $my = 1 - ax$. So, by definition, we have $ax \equiv 1 \mod m$. □

Theorem 6.22 (Chinese Remainder Theorem)**.** *If* m_1 *and* m_2 *are relatively prime, then the system of congruence relations:*

$$x \equiv r_1 \mod m_1$$
$$x \equiv r_2 \mod m_2$$

has a solution $x_0 \in \mathbb{Z}$*. Moreover, any two solutions are congruent modulo* m_1m_2*, and any integer which is congruent to* x_0 *modulo* m_1m_2 *is also a solution.*

Remark. *In other words, the system of two congruence relations is equivalent to a single congruence relation:*

$$x \equiv r \mod m_1 m_2$$

for some $r \in \mathbb{Z}$.

Applying this process repeatedly, a system of congruence relations of the form:

$$\begin{aligned} x &\equiv r_1 \mod m_1 \\ x &\equiv r_2 \mod m_2 \\ &\vdots \\ x &\equiv r_l \mod m_l \end{aligned}$$

where the m_i*'s are pairwise coprime, is equivalent to a single relation of the form:*

$$x \equiv r \mod m_1 m_2 \cdots m_l$$

for some $r \in \mathbb{Z}$.

Proof. Since m_1 and m_2 are relatively prime, by Theorem 6.21 there exists $n \in \mathbb{Z}$ such that $m_1 n \equiv 1 \mod m_2$. Let $x = m_1 n(r_2 - r_1) + r_1$.

Since:

$$m_1 n(r_2 - r_1) \equiv 0 \mod m_1,$$

we have:

$$x \equiv r_1 \mod m_1.$$

Moreover, since $m_1 n \equiv 1 \mod m_2$, we have:

$$x = m_1 n(r_2 - r_1) + r_1 \equiv r_2 - r_1 + r_1 \equiv r_2 \mod m_2.$$

This shows that the system of congruence relations has at least one solution.

If x' is another solution to the system, then:

$$\begin{aligned} x - x' &\equiv r_1 - r_1 \equiv 0 \mod m_1, \\ x - x' &\equiv r_2 - r_2 \equiv 0 \mod m_2. \end{aligned}$$

So, $m_1 | (x - x')$ and $m_2 | (x - x')$. Since, m_1, m_2 are relatively prime, by a previous result we conclude that $m_1 m_2 | (x - x')$. In other words, $x \equiv x' \mod m_1 m_2$.

Conversely, for any integer k, it is clear $x' = x + m_1 m_2 k$ is also a solution provided that x is a solution.

Hence, the solution set to the system of congruence relations may be described by:

$$x \equiv x_0 \mod m_1 m_2,$$

where x_0 is any particular solution to the system. □

Note. The proof of the Chinese Remainder Theorem as written above is complete. However, it is worthwhile to explain how we come up with the solution $x = m_1 n(r_2 - r_1) + r_1$ in the first place.

Heuristically, the solution may be arrived at as follows: For any $q \in \mathbb{Z}$, $x = m_1 q + r_1$ is a solution to the first congruence relation. We want to find q such that $m_1 q + r_1$ is also a solution to the second congruence relation, that is:

$$m_1 q + r_1 \equiv r_2 \mod m_2$$

or, equivalently,

$$m_1 q \equiv r_2 - r_1 \mod m_2. \tag{$*$}$$

Noting that there exists an $n \in \mathbb{Z}$ such that $m_1 n \equiv 1 \mod m_2$, the congruence relation $(*)$ is equivalent to:

$$q \equiv n(r_2 - r_1) \mod m_2.$$

Hence, $x = m_1 q + r_1$ is a solution to the system of congruence relations if and only if q is of the form $m_2 l + n(r_2 - r_1)$, where $l \in \mathbb{Z}$. In particular, $l = 0$ gives $q = n(r_2 - r_1)$. Hence, $x = m_1 n(r_2 - r_1) + r_1$ is a solution.

Example 6.23. *Solve the following system of congruence relations:*

$$x \equiv 3 \mod 34 \tag{6.1}$$
$$x \equiv -1 \mod 27 \tag{6.2}$$

The relation (6.1) *holds if and only if:*

$$x = 34s + 3$$

for some $s \in \mathbb{Z}$*.*

For any such x*, the relation* (6.2) *holds if and only if:*

$$34s + 3 \equiv -1 \mod 27,$$

or equivalently:

$$34s \equiv -4 \mod 27. \tag{6.3}$$

Since $gcd(34, 27) = 1$*, by Theorem 6.21 there exists* $a \in \mathbb{Z}$ *such that* $a \cdot 34 \equiv 1 \mod 27$*. To find* a*, we perform the Euclidean Algorithm on* 34 *and* 27*:*

$$34 = 27 \cdot 1 + 7$$
$$27 = 7 \cdot 3 + 6$$
$$7 = 6 \cdot 1 + 1$$
$$6 = 1 \cdot 6 + 0$$

Working backwards from the last equation, we see that:

$$1 = 34(4) + 27(-5)$$

Hence:

$$27|(1 - 34 \cdot 4)$$

That is, $34 \cdot 4 \equiv 1 \mod 27$. *So, we may take* $a = 4$.

Multiplying both sides of (6.3) *by* $a = 4$, *we see that* (6.3) *holds if and only if:*

$$s \equiv -16 \mod 27,$$

which is equivalent to:

$$s \equiv 11 \mod 27.$$

Since the relation above holds if and only if $s = 27t + 11$ *for some* $t \in \mathbb{Z}$, *we conclude that* $x \in \mathbb{Z}$ *is a solution to our system of congruence relations if and only if:*

$$x = 34s + 3 = 34(27t + 11) + 3 = (34)(27)t + 377$$

for some $t \in \mathbb{Z}$. *More concisely, the solution set to the system of congruence relations is represented by the single relation:*

$$x \equiv 377 \mod 34 \cdot 27$$

Exercise 6.24. *1.* **WeBWorK**

2. **WeBWorK**

3. **WeBWorK**

4. **WeBWorK**

5. **WeBWorK**

6. **WeBWorK**

7. **WeBWorK**

8. **WeBWorK**

9. **WeBWorK**

10. **WeBWorK**

11. **WeBWorK**

12. **WeBWorK**

13. **WeBWorK**

14. **WeBWorK**

MATH 2070A Week 7

Polynomials, Rings

7.1 Polynomials with Rational Coefficients

Notation:

$$\begin{aligned}\mathbb{Q} &= \text{Set of rational numbers}\\ \mathbb{Q}[x] &= \text{Set of polynomials with rational coefficients}\\ &= \{a_0 + a_1x + \cdots + a_nx^n | n \in \mathbb{Z}_{\geq 0}, a_i \in \mathbb{Q}\}\end{aligned}$$

Theorem 7.1 (Division Theorem for Polynomials with Rational Coefficients)**.** *For all $f, g \in \mathbb{Q}[x]$, such that $f \neq 0$, there exist unique $q, r \in \mathbb{Q}[x]$, satisfying $\deg r < \deg f$, such that $g = fq + r$.*

Proof. We first prove the existence of q and r, via induction on the degree of g. The base step corresponds to the case $\deg g < \deg f$. In this case, the choice $q = 0$, $r = g$ works, since $g = f \cdot 0 + g$, and $\deg r = \deg g < \deg f$.

Now, we establish the inductive step. Let f be fixed. Given g, suppose for all g' with $\deg g' < \deg g$, there exist $q', r' \in \mathbb{Q}[x]$ such that $g' = fq' + r'$, with $\deg r' < \deg f$. We want to show that there exist q, r such that $g = fq + r$, with $\deg r < \deg f$.

Suppose $g = a_0 + a_1x + \cdots + a_mx^m$ and $f = b_0 + b_1x + \cdots + b_nx^n$, where $a_m, b_n \neq 0$. We may assume that $m \geq n$, since the case $m < n$ (i.e. $\deg g < \deg f$) has already been proved.

Consider the polynomial:

$$g' = g - \frac{a_m}{b_n}x^{m-n}f.$$

Then, $\deg g' < \deg g$, and by the induction hypothesis we have:

$$g' = fq' + r'$$

for some $q', r' \in \mathbb{Q}[x]$ such that $\deg r' < \deg f$.

Hence,

$$g - \frac{a_m}{b_n} x^{m-n} f = g' = fq' + r',$$

which implies that:

$$g = f\left(q' + \frac{a_m}{b_n} x^{m-n}\right) + r'$$

This establishes the existence of the quotient $q = q' + \frac{a_m}{b_n} x^{m-n}$ and the remainder $r = r'$.

Now, we prove the uniqueness of q and r. Suppose $g = fq + r = fq' + r'$, where $q, q', r, r' \in \mathbb{Q}[x]$, with $\deg r, \deg r' < \deg f$. We have:

$$fq + r = fq' + r',$$

which implies that:

$$\deg f(q - q') = \deg(r' - r) < \deg f.$$

The above inequality can hold only if $q = q'$, which in turn implies that $r' = r$. It follows that the quotient q and the remainder r are unique. □

Definition 7.2. *Given $f, g \in \mathbb{Q}[x]$, a* **Greatest Common Divisor** *d of f and g is a polynomial in $\mathbb{Q}[x]$ which satisfies the following two properties:*

1. *d divides both f and g.*
2. *For any $e \in \mathbb{Q}[x]$ which divides both f and g, we have $\deg e \leq \deg d$.*

Claim 7.3. *If $g = fq + r$, and d is a GCD of g and f, then d is a GCD of f and r.*

Proof. See the proof of Lemma 6.2 . □

Corollary 7.4. *The Euclidean Algorithm applies to $\mathbb{Q}[x]$.*

Namely: Suppose $\deg g \geq \deg f$. let $g_0 = g$, $f_0 = f$, and let r_0 be the unique polynomial in $\mathbb{Q}[x]$ such that:

$$g_0 = f_0 q_0 + r_0, \quad \deg r_0 < \deg f_0,$$

for some $q_0 \in \mathbb{Q}[x]$.

For $k > 0$, let:

$$g_k = f_{k-1}, \quad f_k = r_{k-1}.$$

Let r_k be the remainder such that:

$$g_k = f_k q_k + r_k,$$

for some $q_k \in \mathbb{Q}[x]$.

Since $\deg r_k < \deg f_k = \deg r_{k-1}$*, we have:*

$$\deg r_0 > \deg r_1 > \deg r_2 > \cdots \geq -\infty$$

(where by convention we let $\deg 0 = -\infty$*).*

Eventually, $r_n = 0$ *for some* n*, and it follows from the previous claim and arguments similar to those used in the case of* $\mathbb{Z}$ *that* r_{n-1} *is a GCD of* f *and* g*.*

Example 7.5. *1. Find a GCD of* $x^5 + 1$ *and* $x^3 + 1$ *in* $\mathbb{Q}[x]$.

$$\begin{aligned} x^5 + 1 &= \left(x^3 + 1\right)\left(x^2\right) + \left(-x^2 + 1\right) \\ x^3 + 1 &= \left(-x^2 + 1\right)(-x) + (x + 1) \\ -x^2 + 1 &= (x + 1)(-x + 1) + (0) \end{aligned}$$

So, a GCD is $x + 1$.

2. Find a GCD of $x^3 - x^2 - x + 1$ *and* $x^3 + 4x^2 + x - 6$ *in* $\mathbb{Q}[x]$.

$$\begin{aligned} x^3 - x^2 - x + 1 &= \left(x^3 + 4x^2 + x - 6\right)(1) + \left(-5x^2 - 2x + 7\right) \\ x^3 + 4x^2 + x - 6 &= \left(-5x^2 - 2x + 7\right)\left(-\frac{1}{5}x - \frac{18}{25}\right) + \left(\frac{24}{25}x - \frac{24}{25}\right) \\ -5x^2 - 2x + 7 &= \left(\frac{24}{25}x - \frac{24}{25}\right)\left(-\frac{125}{24}x - \frac{175}{24}\right) + (0) \end{aligned}$$

So, a GCD is $\frac{24}{25}x - \frac{24}{25}$*, and so is* $x - 1$.

Corollary 7.6 (Bézout's Identity for Polynomials)**.** *For any* $f, g \in \mathbb{Q}[x]$ *which are not both zero, and* d *a GCD of* f *and* g*, there exist* $u, v \in \mathbb{Q}[x]$ *such that:*

$$d = fu + gv.$$

Example 7.7. *In Example 7.5, we have:*

$$\begin{aligned} (x + 1) &= \left(x^3 + 1\right) - \left(-x^2 + 1\right)(-x) \\ &= \left(x^3 + 1\right) - \left(\left(x^5 + 1\right) - \left(x^3 + 1\right)\left(x^2\right)\right)(-x) \\ &= \Big(x\Big)\Big(x^5 + 1\Big) + \Big(-x^3 + 1\Big)\Big(x^3 + 1\Big) \end{aligned}$$

7.2 Factorization of Polynomials

Definition 7.8. *A polynomial p in $\mathbb{Q}[x]$ is* **irreducible** *if it satisfies the following conditions:*

1. $\deg p > 0$,
2. *if $p = ab$ for some $a, b \in \mathbb{Q}[x]$, then either a or b is a constant.*

Claim 7.9. *If $p \in \mathbb{Q}[x]$ is irreducible and $p|f_1 f_2$, where $f_1, f_2 \in \mathbb{Q}[x]$, then $p|f_1$ or $p|f_2$.*

Proof. Suppose p does not divide f_2, then the only common divisors of p and f_2 are constant polynomials. In particular, 1 is a GCD of p and f_2. Then, by Bézout's Identity for Polynomials , there exist $u, v, \mathbb{Q}[x]$ such that $1 = pu + f_2 v$. We have:

$$f_1 = puf_1 + f_1 f_2 v.$$

Since p divides the right-hand side of the above equation, it must divide f_1. □

Theorem 7.10. *A polynomial in $\mathbb{Q}[x]$ of degree greater than zero is either irreducible or a product of irreducibles.*

Proof. Suppose there is a nonempty set of polynomials of degree > 0 which are neither irreducible nor products of irreducibles. Let p be an element of this set which has the least degree. Since p is not irreducible, there are $a, b \in \mathbb{Q}[x]$ of degrees > 0 such that $p = ab$. But, a, b, having degrees strictly less than $\deg p$, must be either irreducible or products of irreducibles. This implies that p is a product of irreducibles, a contradiction. □

Remark: Compare this proof with that of Part 1 of the Fundamental Theorem of Arithmetic (The Fundamental Theorem of Arithmetic).

Theorem 7.11 (Unique Factorization for Polynomials)**.** *For any $p \in \mathbb{Q}[x]$ of degree > 0, if:*

$$p = f_1 f_2 \cdots f_n = g_1 g_2 \cdots g_m,$$

where f_i, g_j are irreducible polynomials in $\mathbb{Q}[x]$, then $n = m$, and the g_j's may be reindexed so that $f_i = \lambda_i g_i$ for some $\lambda_i \in \mathbb{Q}$, for $i = 1, 2, \ldots, n$.

Proof. **Exercise** . See the proof of Part 2 of The Fundamental Theorem of Arithmetic). □

7.3 Rings

7.3.1 Definition of a Ring

Definition 7.12. *A* **ring** R *(or* $(R, +, \times)$*) is a set equipped with two operations:*

$$\times, + : R \times R \to R$$

which satisfy the following properties:

1. *Properties of* $+$*:*
   (a) *Commutativity:* $a + b = b + a$*,* $\forall a, b \in R$*.*
   (b) *Associativity:* $a + (b + c) = (a + b) + c$*.*
   (c) *There is an element* $0 \in R$ *(called the* **additive identity element** *), such that* $a + 0 = a$ *for all* $a \in R$*.*
   (d) *Every element of* R *has an additive inverse; namely: For all* $a \in R$*, there exists an element of* R*, usually denoted* $-a$*, such that* $a + (-a) = 0$*.*
2. *Properties of* $\times$*:*
   (a) *Associativity:* $a(bc) = (ab)c$*.*
   (b) *There is an element* $1 \in R$ *(called the* **multiplicative identity element** *), such that* $1 \times a = a \times 1 = a$ *for all* $a \in R$*.*
3. *Distributativity:*
   (a) $a \times (b + c) = a \times b + a \times c$*, for all* $a, b, c \in R$*.*
   (b) $(a + b) \times c = a \times c + b \times c$*, for all* $a, b, c \in R$*.*

Note:

1. For convenience's sake, we often write ab for $a \times b$.
2. In the definition, commutativity is required of addition, but not of multiplication.
3. Every element has an additive inverse, but *not necessarily* a multiplicative inverse. That is, there may be an element $a \in R$ such that $ab \neq 1$ for all $b \in R$.

Example 7.13. *The following sets, equipped with the usual operations of addition and multiplication, are rings:*

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

2. $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ *(Polynomials with integer, rational, real coefficients, respectively.)*

3. $$\begin{aligned}\mathbb{Q}[\sqrt{2}] &= \{\sum_{k=0}^{n} a_k(\sqrt{2})^k \mid a_k \in \mathbb{Q}, n \in \mathbb{Z}_{\geq 0}\} \\ &= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.\end{aligned}$$

4. $M_n(\mathbb{R})$, *the set of* $n \times n$ *real matrices,* $n \in \mathbb{N}$.

5. *For a fixed* n, *the set of* $n \times n$ *matrices with integer coefficients.*

6. $C[0,1] = \{f : [0,1] \to \mathbb{R} \mid f$ *is continuous.*$\}$

The following sets, under the usual operations of addition and multiplication, are not rings:

1. $\mathbb{N}$, *no additive identity element, i.e. no 0.*

2. $\mathbb{N} \cup \{0\}$, *nonzero elements have no additive inverses.*

3. $\mathrm{GL}(n, \mathbb{R})$, *the set of* $n \times n$ *invertible real matrices,* $n \in \mathbb{N}$.

Claim 7.14. *In a ring* R, *there is a unique additive identity element and a unique multiplicative identity element.*

Proof. Suppose there is an element $0' \in R$ such that $0' + r = r$ for all $r \in R$, then in particular $0' + 0 = 0$.

Since 0 is an additive identity, we have $0' + 0 = 0'$. So, $0' = 0$.

Suppose there is an element $1' \in R$ such that $1'r = r$ or all $r \in R$,

then in particular $1' \cdot 1 = 1$.

But $1' \cdot 1 = 1'$ since 1 is a multiplicative identity element, so $1' = 1$. □

Exercise 7.15. *Prove that: For any* r *in a ring* R, *its additive inverse* $-r$ *is unique. That is, if* $r + r' = r + r'' = 0$, *then* $r' = r''$.

7.3.2 WeBWorK

1. **WeBWorK**

2. **WeBWorK**

Claim 7.16. *For all elements r in a ring R, we have $0r = r0 = 0$.*

Proof. By distributativity,

$$0r = (0 + 0)r = 0r + 0r.$$

Adding $-0r$ (additive inverse of $0r$) to both sides, we have:

$$0 = (0r + 0r) + (-0r) = 0r + (0r + (-0r)) = 0r + 0 = 0r.$$

The proof of $r0 = 0$ is similar and we leave it as an **exercise** . □

Claim 7.17. *For all elements r in a ring, we have $(-1)(-r) = (-r)(-1) = r$.*

Proof. We have:

$$0 = 0(-r) = (1 + (-1))(-r) = -r + (-1)(-r).$$

Adding r to both sides, we obtain

$$r = r + (-r + (-1)(-r)) = (r + -r) + (-1)(-r) = (-1)(-r).$$

We leave it as an **exercise** to show that $(-r)(-1) = r$. □

Exercise 7.18. *Show that: For all r in a ring R, we have:*

$$(-1)r = r(-1) = -r.$$

Exercise 7.19. *Show that: If R is a ring in which $1 = 0$, then $R = \{0\}$. That is, it has only one element.*

(We call such an R the **zero ring** *.)*

MATH 2070A Week 8

Rings, Integral Domains, Fields

8.1 Integral Domains, Units

Definition 8.1. *A ring R is said to be* **commutative** *if $ab = ba$ for all $a, b \in R$.*

Example 8.2. *For a fixed natural number $n > 1$, the ring of $n \times n$ matrices with integer coefficients, under the usual operations of addition and multiplication, is not commutative.*

Example 8.3. *Let m be a natural number greater than 1. Let $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. Recall that for any integer $n \in \mathbb{Z}$, there exists a unique $\overline{n} \in \mathbb{Z}_m$, such that $n \equiv \overline{n} \mod m$. More precisely, $\overline{n}$ is the remainder of the division of of n by m: $n = mq + r$. We equip $\mathbb{Z}_m$ with addition $+_m$ and multiplication $\times_m$ defined as follows: For $a, b \in \mathbb{Z}_m$, let:*

$$a +_m b = \overline{a + b},$$
$$a \times_m b = \overline{a \cdot b},$$

where the addition and multiplication on the right are the usual addition and multiplication for integers.

Claim 8.4. *With addition and multiplication thus defined, $\mathbb{Z}_m$ is a commutative ring.*

Proof. 1. For $a, b \in \mathbb{Z}_m$, we have $a +_m b = \overline{a + b} = \overline{b + a} = b +_m a$, since addition for integers is commutative. So, $+_m$ is commutative.

2. For any $r_1, r_2 \in \mathbb{Z}$, by Claim 6.17 and Theorem 6.19 , we have

$$r_1 \equiv \overline{r_1} \mod m, \quad r_2 \equiv \overline{r_2} \mod m,$$

and:

$$\overline{r_1 + r_2} \equiv r_1 + r_2 \equiv \overline{r_1} + \overline{r_2} \equiv \overline{\overline{r_1} + \overline{r_2}} \mod m.$$

For $a, b, c \in \mathbb{Z}_m$, we have:

$$\begin{aligned} a +_m (b +_m c) &= a +_m \overline{b + c} \\ &= \overline{a + \overline{b + c}} \\ &= \overline{\overline{a} + \overline{b + c}} \\ &= \overline{a + (b + c)} \end{aligned}$$

But $a+(b+c)$ is equal to $(a+b)+c$, since addition for integers is associative. Hence, the above expression is equal to:

$$\begin{aligned} \overline{(a + b) + c} &= \overline{\overline{(a + b)} + \overline{c}} \\ &= \overline{\overline{a + b} + c} \\ &= \overline{(a +_m b) + c} \\ &= (a +_m b) +_m c. \end{aligned}$$

We conclude that $+_m$ is associative.

---

3. **Exercise:** We can take 0 to be the additive identity element.

4. For each nonzero element $a \in \mathbb{Z}_m$, we can take the additive inverse of a to be $m - a$. Indeed, $a +_m (-a) = \overline{a + (m - a)} = \overline{m} = 0$.

5. By the same reasoning used in the case of addition, for $r_1, r_2 \in \mathbb{Z}$, we have

$$\overline{r_1 r_2} \equiv r_1 r_2 \equiv \overline{r_1} \cdot \overline{r_2} \equiv \overline{\overline{r_1} \cdot \overline{r_2}} \mod m.$$

For $a, b, c \in \mathbb{Z}_m$, we have:

$$a \times_m (b \times_m c) = a \times_m \overline{bc} = \overline{\overline{a} \cdot \overline{bc}} = \overline{a(bc)},$$

which by the associativity of multiplication for integers is equal to:

$$\overline{(ab)c} = \overline{\overline{ab} \cdot \overline{c}} = \overline{ab} \times_m c = (a \times_m b) \times_m c.$$

So, $\times_m$ is associative.

6. **Exercise:** We can take 1 to be the multiplicative identity.

7. For $a, b \in \mathbb{Z}_m$, $a \times_m b = \overline{a \cdot b} = \overline{b \cdot a} = b \times_m a$. So $\times_m$ is commutative.

8. Lastly, we need to prove distributativity. For $a, b, c \in \mathbb{Z}_m$, we have:

$$\begin{aligned} a \times_m (b +_m c) &= \overline{\overline{a} \cdot \overline{b + c}} \\ &= \overline{a \cdot (b + c)} \\ &= \overline{ab + ac} \\ &= \overline{\overline{ab} + \overline{ac}} \\ &= a \times_m b +_m a \times_m c. \end{aligned}$$

   It now follows from the distributativity from the left, proven above, and the commutativity of $\times_m$, that distributativity from the right also holds:

$$(a +_m b) \times_m c = a \times_m c + b \times_m c.$$

□

Definition 8.5. *A nonzero commutative ring R is an* **integral domain** *if the product of two nonzero elements is always nonzero.*

Definition 8.6. *A nonzero element r in a ring R is called a* **zero divisor** *if there exists nonzero $s \in R$ such that $rs = 0$ or $sr = 0$.*

Note. A nonzero commutative ring R is an integral domain if and only if it has no zero divisors.

Example 8.7. *Since $2, 3 \neq 0$ in $\mathbb{Z}_6$, but $2 \times_6 3 = \bar{6} = 0$, the ring $\mathbb{Z}_6$ is not an integral domain.*

Claim 8.8. *A commutative ring R is an integral domain if and only if the* **cancellation law** *holds for multiplication. That is: Whenever $ca = cb$ and $c \neq 0$, we have $a = b$.*

Proof. Suppose R is an integral domain.

If $ca = cb$, then by distributativity $c(a - b) = c(a + -b) = 0$.

Since R is an integral domain, we have either $c = 0$ or $a - b = 0$.

So, if $c \neq 0$, we must have $a = b$.

Conversely, suppose cancellation law holds. It suffices to show that whenever we have $a, b \in R$ such that $ab = 0$ and $a \neq 0$, then we must have $b = 0$.

By a previous result we know that $0 = a0$. So, $ab = a0$, which by the cancellation law implies that $b = 0$. □

Note. If every nonzero element of a commutative ring has a multiplicative inverse, then that ring is an integral domain:

$$ca = cb \implies c^{-1}ca = c^{-1}cb \implies a = b.$$

However, a nonzero element of an integral domain does not necessarily have a multiplicative inverse.

Example 8.9. *The ring $\mathbb{Z}$ is an integral domain, for the product of two nonzero integers is nonzero. So, the cancellation law holds for $\mathbb{Z}$, but the only nonzero elements in $\mathbb{Z}$ which have multiplicative inverses are ± 1.*

Example 8.10. *The ring $\mathbb{Q}[x]$ is an integral domain.*

Exercise 8.11. *Show that: For $m > 1$, $\mathbb{Z}_m$ is an integral domain if and only if m is a prime.*

Example 8.12. *Consider $R = C[-1, 1]$, the ring of all continuous functions on $[-1, 1]$, equipped with the usual operations of addition and multiplication for functions.*

Let:

$$f(x) = \begin{cases} -x, & -1 \leq x \leq 0, \\ 0, & 0 < x \leq 1. \end{cases} \quad , \quad g(x) = \begin{cases} 0, & -1 \leq x \leq 0, \\ x, & 0 < x \leq 1. \end{cases}$$

Then f and g are nonzero elements of R, but $fg = 0$.

So R is not an integral domain.

Definition 8.13. *We say that an element $r \in R$ is a* **unit** *if it has a multiplicative inverse; i.e. there is an element $r^{-1} \in R$ such that $rr^{-1} = r^{-1}r = 1$.*

Example 8.14. *Consider $4 \in \mathbb{Z}_{25}$. Since $4 \cdot 19 = 76 \equiv 1 \mod 25$, we have $4^{-1} = 19$ in $\mathbb{Z}_{25}$. So, 4 is a unit in $\mathbb{Z}_{25}$.*

On the other hand, consider $10 \in \mathbb{Z}_{25}$. Since $10 \cdot 5 = 50 \equiv 0 \mod 25$, we have $10 \cdot 5 = 0$ in $\mathbb{Z}_{25}$. If 10^{-1} exists, then by the associativity of multiplication, we would have:

$$5 = (10^{-1} \cdot 10) \cdot 5 = 10^{-1} \cdot (10 \cdot 5) = 10^{-1} \cdot 0 = 0,$$

a contradiction. So, 10 is not a unit in $\mathbb{Z}_{25}$.

Claim 8.15. *Let $m \in \mathbb{N}$ be greater than one. Then, $r \in \mathbb{Z}_m$ is a unit if and only if r and m are relatively prime; i.e. $gcd(r, m) = 1$.*

Proof. Suppose $r \in \{0, 1, 2, \ldots, m-1\}$ is a unit in $\mathbb{Z}_m$, then there exists $r^{-1} \in \mathbb{Z}_m$ such that $r \cdot r^{-1} \equiv 1 \mod m$.

In other words, there exists $x \in \mathbb{Z}$ such that $r \cdot r^{-1} - 1 = mx$, or $r \cdot r^{-1} - mx = 1$. This implies that if there is an integer d such that $d|r$ and $d|m$, then d must also divide 1. Hence, the GCD of r and m is 1.

Conversely, if $gcd(r, m) = 1$, then there exists $x, y \in \mathbb{Z}$ such that $rx + my = 1$.

It follows that $r^{-1} = \overline{x}$ is a multiplicative inverse of r. Here, $\overline{x} \in \mathbb{Z}_m$ is the remainder of the division of x by m. □

Corollary 8.16. *For p prime, every nonzero element of $\mathbb{Z}_p$ is a unit.*

Example 8.17. *The only units of $\mathbb{Z}$ are ± 1.*

Example 8.18. *Let R be the ring of all real-valued functions on $\mathbb{R}$. Then, any function $f \in R$ satisfying $f(x) \neq 0$, $\forall x$, is a unit.*

@eg@newcol Let R be the ring of all continuous real-valued functions on $\mathbb{R}$, then $f \in R$ is a unit if and only if it is either strictly positive or strictly negative. @endcol@end

Claim 8.19. *The only units of $\mathbb{Q}[x]$ are nonzero constants.*

Proof. Given any $f \in \mathbb{Q}[x]$ such that $\deg f > 0$, for all nonzero $g \in \mathbb{Q}[x]$ we have

$$\deg fg \geq \deg f > 0 = \deg 1;$$

hence, $fg \neq 1$. If $g = 0$, then $fg = 0 \neq 1$. So, f has no multiplicative inverse.

If f is a nonzero constant, then $f^{-1} = \frac{1}{f}$ is a constant polynomial in $\mathbb{Q}[x]$, and $f \cdot \frac{1}{f} = \frac{1}{f} \cdot f = 1$. So, f is a unit.

Finally, if $f = 0$, then $fg = 0 \neq 1$ for all $g \in \mathbb{Q}[x]$, so the zero polynomial has no multiplicative inverse. □

8.1.1 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**
5. **WeBWorK**

8.2 Fields

Definition 8.20. *A* **field** *is a commutative ring, with* $1 \neq 0$*, in which every nonzero element is a unit.*

In other words, a nonzero commutative ring F is a field if and only if every nonzero element $r \in F$ has a multiplicative inverse r^{-1}, i.e. $rr^{-1} = r^{-1}r = 1$.

Since every nonzero element of a field is a unit, a field is necessarily an integral domain, but an integral domain is not necessarily a field. For example $\mathbb{Z}$ is an integral domain which is not a field.

Example 8.21. *1.* $\mathbb{Q}$*,* $\mathbb{R}$ *are fields.*

2. *For* $m \in \mathbb{N}$*, it follows from a previous result that* $\mathbb{Z}_m$ *is a field if and only if* m *is prime.*

   Notation *For* p *prime, we often denote the field* $\mathbb{Z}_p$ *by* $\mathbb{F}_p$*.*

Claim 8.22. *Equipped with the usual operations of addition and multiplications for real numbers,* $F = \mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ *is a field.*

Proof. Observe that: $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$ lies in F, and $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in F$. Hence, addition and multiplication for real numbers are well-defined operations on F. As operations on $\mathbb{R}$, they are commutative, associative, and satisfy distributativity; therefore, as F is a subset of $\mathbb{R}$, they also satisfy these properties as operations on F.

It is clear that 0 and 1 are the additive and multiplicative identities of F. Given $a + b\sqrt{2} \in F$, where $a, b \in \mathbb{Q}$, it is clear that its additive inverse $-a - b\sqrt{2}$ also lies in F. Hence, F is a commutative ring.

To show that F is a field, for every nonzero $a + b\sqrt{2}$ in F, we need to find its multiplicative inverse. As an element of the field $\mathbb{R}$, the multiplicative inverse of $a + b\sqrt{2}$ is:

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

It remains to show that this number lies in F. Observe that:

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$

We claim that $a^2 - 2b^2 \neq 0$.

Suppose $a^2 - 2b^2 = 0$, then either (i) $a = b = 0$, or (ii) $b \neq 0$, $\sqrt{2} = |a/b|$.

Since we have assumed that $a + b\sqrt{2}$ is nonzero, case (i) cannot hold.

But case (ii) also cannot hold because $\sqrt{2}$ is known to be irrational. Hence $a^2 - 2b^2 \neq 0$, and:

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2},$$

which lies in F. □

Claim 8.23. *All finite integral domains are fields.*

Proof. Let R be an integral domain with n elements, where n is finite. Write $R = \{a_1, a_2, \ldots, a_n\}$.

We want to show that for any nonzero element $a \neq 0$ in R, there exists i, $1 \leq i \leq n$, such that a_i is the multiplicative inverse of a.

Consider the set $S = \{aa_1, aa_2, \ldots, aa_n\}$. Since R is an integral domain, the cancellation law holds. In particular, since $a \neq 0$, we have $aa_i = aa_j$ if and only if $i = j$.

The set S is therefore a subset of R with n distinct elements, which implies that $S = R$.

In particular, $1 = aa_i$ for some i. This a_i is the multiplicative inverse of a. □

8.2.1 Field of Fractions

An integral domain fails to be a field precisely when there is a nonzero element with no multiplicative inverse. The ring $\mathbb{Z}$ is such an example, for $2 \in \mathbb{Z}$ has no multiplicative inverse.

But any nonzero $n \in \mathbb{Z}$ has a multiplicative inverse $\frac{1}{n}$ in $\mathbb{Q}$, which is a field.

So, a question one could ask is, can we "enlarge" a given integral domain to a field, by formally adding multiplicative inverses to the ring?

An Equivalence Relation

Given an integral domain R (commutative, with $1 \neq 0$). We consider the set: $R \times R_{\neq 0} := \{(a, b) : a, b \in R, b \neq 0\}$. We define a relation $\equiv$ on $R \times R_{\neq 0}$ as follows:

$$(a, b) \equiv (c, d) \text{ if } ad = bc.$$

Lemma 8.24. *The relation $\equiv$ is an equivalence relation.*

In other words, the relation $\equiv$ is:

1. **Reflexive:** $(a, b) \equiv (a, b)$ *for all* $(a, b) \in R \times R_{\neq 0}$
2. **Symmetric:** *If* $(a, b) \equiv (c, d)$*, then* $(c, d) \equiv (a, b)$.
3. **Transitive:** *If* $(a, b) \equiv (c, d)$ *and* $(c, d) \equiv (e, f)$*, then* $(a, b) \equiv (e, f)$.

Proof. **Exercise.** □

Due to the properties (reflexive, symmetric, transitive), of an equivalence relation, the equivalent classes form a **partition** of S. Namely, equivalent classes of non-equivalent elements are disjoint:

$$[s] \cap [t] = \varnothing$$

if $s \not\sim t$; and the union of all equivalent classes is equal to S:

$$\bigcup_{s \in S} [s] = S.$$

Definition 8.25. *Given an equivalence relation $\sim$ on a set S, the* **quotient set** *$S/\sim$ is the set of all equivalence classes of S, with respect to $\sim$.*

We now return to our specific situation of $R \times R_{\neq 0}$, with $\equiv$ defined as above. We define addition $+$ and multiplication $\cdot$ on $R \times R_{\neq 0}$ as follows:

$$(a, b) + (c, d) := (ad + bc, bd)$$
$$(a, b) \cdot (c, d) := (ac, bd)$$

Claim 8.26. *Suppose $(a, b) \equiv (a', b')$ and $(c, d) \equiv (c', d')$, then:*

1. $(a, b) + (c, d) \equiv (a', b') + (c', d')$.
2. $(a, b) \cdot (c, d) \equiv (a', b') \cdot (c', d')$.

Proof. By definition, $(a, b) + (c, d) = (ad + bc, bd)$, and $(a', b') + (c', d') = (a'd' + b'c', b'd')$. Since by assumption $ab' = a'b$ and $cd' = c'd$,

we have:

$$(ad + bc)b'd' = adb'd' + bcb'd' = a'bdd' + c'dbb' = (a'd' + b'c')bd;$$

hence, $(a, b) + (c, d) \equiv (a', b') + (c', d')$.

For multiplication, by definition we have $(a, b) \cdot (c, d) = (ac, bd)$ and $(a', b') \cdot (c', d') = (a'c', b'd')$.

Since

$$acb'd' = ab'cd' = a'bc'd = a'c'bd,$$

we have $(a, b) \cdot (c, d) \equiv (a', b') \cdot (c', d')$. □

Let:

$$\mathrm{Frac}(R) := (R \times R_{\neq 0})/\equiv,$$

and define $+$ and $\cdot$ on $\mathrm{Frac}(R)$ as follows:

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$
$$[(a, b)] \cdot [(c, d)] = [(ac, bd)]$$

Corollary 8.27. *$+$ and $\cdot$ thus defined are well-defined binary operations on $\mathrm{Frac}(R)$.*

In other words, we get the same output in $\mathrm{Frac}(R)$ regardless of the choice of representatives of the equivalence classes.

Claim 8.28. *The set $\mathrm{Frac}(R)$, equipped with $+$ and $\cdot$ defined as above, forms a field, with additive identity $0 = [(0,1)]$ and multiplicative identity $1 = [(1,1)]$. The multiplicative inverse of a nonzero element $[(a,b)] \in \mathrm{Frac}(R)$ is $[(b,a)]$.*

Proof. **Exercise.** □

Definition 8.29. *$\mathrm{Frac}(R)$ is called the* **Fraction Field** *of R.*

Note. $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, if we identify $a/b \in \mathbb{Q}$, $a, b \in \mathbb{Z}$, with $[(a,b)] \in \mathrm{Frac}(\mathbb{Z})$.

8.2.2 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**
5. **WeBWorK**
6. **WeBWorK**
7. **WeBWorK**
8. **WeBWorK**
9. **WeBWorK**
10. **WeBWorK**

MATH 2070A Week 9

Ring Homomorphisms

9.1 Homomorphisms

Definition 9.1. *Let $(A, +_A, \cdot_A)$, $(B, +_B, \cdot_B)$ be rings. A* **ring homomorphism** *from A to B is a map $\phi : A \to B$ with the following properties:*

1. $\phi(1_A) = 1_B$.
2. $\phi(a_1 +_A a_2) = \phi(a_1) +_B \phi(a_2)$, *for all* $a_1, a_2 \in A$.
3. $\phi(a_1 \cdot_A a_2) = \phi(a_1) \cdot_B \phi(a_2)$, *for all* $a_1, a_2 \in A$.

Note that if $\phi : A \to B$ is a homomorphism, then:

1. $$1 = \phi(1) = \phi(1 + 0) = \phi(1) + \phi(0) = 1 + \phi(0),$$
   which implies that $\phi(0) = 0$.
2. For all $a \in A$, $0 = \phi(0) = \phi(-a + a) = \phi(-a) + \phi(a)$, which implies that $\phi(-a) = -\phi(a)$.
3. If u is a unit in A, then $1 = \phi(u \cdot u^{-1}) = \phi(u)\phi(u^{-1})$, and $1 = \phi(u^{-1} \cdot u) = \phi(u^{-1})\phi(u)$; which implies that $\phi(u)$ is a unit, with $\phi(u)^{-1} = \phi(u^{-1})$.

Example 9.2. *The map $\phi : \mathbb{Z} \to \mathbb{Q}$ defined by:*

$$\phi(n) = \frac{n}{1}, \quad n \in \mathbb{Z},$$

is a homomorphism, since:

1. $\phi(1) = \frac{1}{1} = 1_{\mathbb{Q}}$,

2. $\phi(n +_{\mathbb{Z}} m) = \frac{m+n}{1} = \frac{n}{1} +_{\mathbb{Q}} \frac{m}{1} = \phi(n) +_{\mathbb{Q}} \phi(m)$.

3. $\phi(n \cdot_{\mathbb{Z}} m) = \frac{mn}{1} = \frac{n}{1} \cdot_{\mathbb{Q}} \frac{m}{1} = \phi(n) \cdot_{\mathbb{Q}} \phi(m)$.

Example 9.3. *Fix an integer m which is larger than 1. For $n \in \mathbb{Z}$, let $\overline{n}$ denote the remainder of the division of n by m. That is:*

$$n = mq + \bar{n}, \quad 0 \leq \bar{n} < m$$

Recall that $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ is a ring, with the addition law defined by:

$$s +_m t = \overline{s + t},$$

and the multiplication law defined by:

$$s \times_m t = \overline{s \cdot t},$$

for all $s, t \in \mathbb{Z}_m$. Here, $+$ and $\cdot$ are the usual addition and multiplication for integers.

Define a map $\phi : \mathbb{Z} \to \mathbb{Z}_m$ as follows:

$$\phi(n) = \overline{n}, \quad \forall n \in \mathbb{Z}.$$

Then, ϕ is a homomorphism.

Proof. 1. $\phi(1) = \overline{1} = 1$,

2. $\phi(s + t) = \overline{s + t} = \overline{\overline{s} + \overline{t}} = \overline{s} +_m \overline{t} = \phi(s) +_m \phi(t)$.

3. $\phi(s \cdot t) = \overline{s \cdot t} = \overline{\overline{s} \cdot \overline{t}} = \overline{s} \times_m \overline{t} = \phi(s) \times_m \phi(t)$.

□

Example 9.4. *For any ring R, define a map $\phi : \mathbb{Z} \to R$ as follows:*

$$\phi(0) = 0;$$

For $n \in \mathbb{N}$,

$$\phi(n) = n \cdot 1_R := \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}};$$

$$\phi(-n) = -n \cdot 1_R := n \cdot (-1_R) = \underbrace{(-1_R) + (-1_R) + \cdots + (-1_R)}_{n \text{ times}}.$$

The map ϕ is a homomorphism.

Proof. **Exercise.** □

Example 9.5. *Let R be a commutative ring. For each element $r \in R$, we may define the* **evaluation map** *$\phi_r : R[x] \to R$ as follows:*

$$\phi_r\left(\sum_{k=0}^{n} a_k x^k\right) = \sum_{k=0}^{n} a_k r^k$$

The map ϕ_r is a ring homomorphism.

Proof. Discussed in class. □

Definition 9.6. *If a ring homomorphism $\phi : A \to B$ is a bijective map, we say that ϕ is an* **isomorphism***, and that A and B are* **isomorphic** *as rings.*

Notation If A and B are isomorphic, we write $A \cong B$.

Claim 9.7. *If $\phi : A \to B$ is an isomorphism, then $\phi^{-1} : B \to A$ is an isomorphism.*

Proof. Since ϕ is bijective, ϕ^{-1} is clearly bijective. It remains to show that ϕ^{-1} is a homomorphism:

1. Since $\phi(1_A) = 1_B$, we have $\phi^{-1}(1_B) = \phi^{-1}(\phi(1_A)) = 1_A$.

2. For all $b_1, b_2 \in B$, we have

$$\begin{aligned}\phi^{-1}(b_1 + b_2) &= \phi^{-1}(\phi(\phi^{-1}(b_1)) + \phi(\phi^{-1}(b_2))) \\ &= \phi^{-1}(\phi(\phi^{-1}(b_1) + \phi^{-1}(b_2))) = \phi^{-1}(b_1) + \phi^{-1}(b_2)\end{aligned}$$

3. For all $b_1, b_2 \in B$, we have

$$\begin{aligned}\phi^{-1}(b_1 \cdot b_2) &= \phi^{-1}(\phi(\phi^{-1}(b_1)) \cdot \phi(\phi^{-1}(b_2))) \\ &= \phi^{-1}(\phi(\phi^{-1}(b_1) \cdot \phi^{-1}(b_2))) = \phi^{-1}(b_1) \cdot \phi^{-1}(b_2)\end{aligned}$$

This shows that ϕ^{-1} is a bijective homomorphism. □

MATH 2070A Week 10

Ideals, Principal Ideal Domains, Quotient Rings

10.1 Ring Homomorphisms - continued

An isomorphism is more than simply a bijective map, for it must preserve algebraic structure.

For example, there is a bijective map $f : \mathbb{Z} \to \mathbb{Q}$, but the two are clearly not isomorphic as rings:

Suppose $\phi : \mathbb{Z} \to \mathbb{Q}$ is an isomorphism. Then, both ϕ and ϕ^{-1} must send units to units.

Consider $2 \in \mathbb{Q}$. Since $\mathbb{Q}$ is a field, the nonzero element 2 is a unit. So $\phi^{-1}(2)$ must be a unit of $\mathbb{Z}$.

But the only units of $\mathbb{Z}$ are ± 1. Since ϕ is an homomorphism, we have $\phi(1) = 1 \neq 2$.

So, we are left with the case $\phi(-1) = 2$. This cannot hold either, since:

$$1 = \phi((-1)(-1)) = \phi(-1)\phi(-1)$$

implies that $\phi(-1)$ could only be $\pm 1 \neq 2$.

So, $\mathbb{Z}$ and $\mathbb{Q}$ cannot be isomorphic.

Theorem 10.1. *The fields* $\mathbb{Q}$ *and* $\mathrm{Frac}(\mathbb{Z})$ *are isomorphic.*

Proof. Define a map $\phi : \mathbb{Q} \to \mathrm{Frac}(\mathbb{Z})$ as follows:

$$\phi(a/b) = [(a, b)], \quad \forall\, a/b \in \mathbb{Q}, a, b \in \mathbb{Z}, b \neq 0.$$

We first need to show that ϕ is well-defined. Namely, suppose $a/b = c/d$ in $\mathbb{Q}$, we need to show that $\phi(a/b) = [(a, b)]$ is equal to $\phi(c/d) = [(c, d)]$.

This is clear, since $a/b = c/d$ implies that $ad = bc$, which by definition of $\mathrm{Frac}(\mathbb{Z})$ implies that $[(a, b)] = [(c, d)]$.

We now show that ϕ is a homomorphism:

1. $\phi(1) = \phi(1/1) = [(1,1)]$, which is indeed the multiplicative identity of $\mathrm{Frac}(\mathbb{Z})$.

2. For $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$, we have:

$$\begin{aligned}\phi(a/b + c/d) = \phi((ad+bc)/(bd)) &= [(ad+bc, bd)] \\ &= [(a,b)] + [(c,d)] = \phi(a/b) + \phi(c/d)\end{aligned}$$

3. For $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$, we have:

$$\begin{aligned}\phi((a/b)(c/d)) = \phi((ac)/(bd)) &= [(ac, bd)] \\ &= [(a,b)] \cdot [(c,d)] = \phi(a/b)\phi(c/d)\end{aligned}$$

Finally, we need to show that ϕ is one-to-one and onto.

Suppose there are $a, b, c, d \in \mathbb{Z}$ such that $\phi(a/b) = \phi(c/d)$. Then, by definition of ϕ we have $[(a,b)] = [(c,d)]$, which implies that $ad = bc$, from which it follows that $a/b = c/d$ as elements of $\mathbb{Q}$. So, ϕ is one-to-one.

Given $[(a,b)] \in \mathrm{Frac}(\mathbb{Z})$, $a, b \in \mathbb{Z}$, $b \neq 0$, it is clear that a/b belongs to $\mathbb{Q}$, and $\phi(a/b) = [(a,b)]$. So ϕ is onto.

Hence, ϕ is a bijective homomorphism. In other words, it is an isomorphism. □

Theorem 10.2. *If F is a field, then $\mathrm{Frac}(F) \cong F$.*

Proof. Define a map $\phi : F \to \mathrm{Frac}(F)$ as follows:

$$\phi(s) = [(s,1)], \quad \forall s \in F.$$

Exercise:

1. Show that ϕ is a homomorphism.

2. Show that ϕ is bijective.

□

Definition 10.3. *The* **kernel** *of a ring homomorphism $\phi : A \to B$ is the set:*

$$\ker \phi := \{a \in A : \phi(a) = 0\}$$

The **image** *of ϕ is the set:*

$$\mathrm{im}\, \phi := \{b \in B : b = \phi(a) \textit{ for some } a \in A\}.$$

Claim 10.4. *A ring homomorphism $\phi : A \to B$ is one-to-one if and only if* $\ker \phi = \{0\}$.

Proof. Suppose ϕ is one-to-one. For any $a \in \ker \phi$, we have $\phi(0) = \phi(a) = 0$, which implies that $a = 0$ since ϕ is one-to-one. Hence, $\ker \phi = \{0\}$.

Suppose $\ker \phi = \{0\}$. If $\phi(a) = \phi(a')$, then $0 = \phi(a) - \phi(a') = \phi(a - a')$, which implies that $a - a' \in \ker \phi = \{0\}$. So, $a - a' = 0$, which implies that $a = a'$. Hence, ϕ is one-to-one. □

Definition 10.5. *An* **ideal** I *in a commutative ring R is a subset of R which satisfies the following properties:*

1. $0 \in I$;
2. *If* $a, b \in I$, *then* $a + b \in I$.
3. *For all* $a \in I$, *we have* $ar \in I$ *for all* $r \in R$.

If an ideal I is a proper subset of R, we say it is a **proper ideal** .

Note. If an ideal I contains 1, then $r = 1 \cdot r \in I$ for all $r \in R$, which implies that $I = R$.

Remark. There is a definition of an **ideal** in the more general case where the ring is not necessarily commutative. It is similar to the definition above, except for one extra condition: ra belongs to I for all $a \in I$, $r \in R$.

Clearly, this general definition coincides with the one above in the special case that the ring is commutative. In this introductory course, unless otherwise noted, we will always discuss ideals in the context of commutative rings.

Example 10.6. *For any commutative ring R, the set $\{0\}$ is an ideal, since $0+0 = 0$, and $0 \cdot r = 0$ for all $r \in R$.*

Example 10.7. *For all $m \in \mathbb{Z}$, the set $I = m\mathbb{Z} := \{mn : n \in \mathbb{Z}\}$ is an ideal:*

1. $0 = m \cdot 0 \in I$;
2. $mn_1 + mn_2 = m(n_1 + n_2) \in I$.
3. *Given $mn \in I$, for all $l \in \mathbb{Z}$, we have $mn \cdot l = m \cdot nl \in I$.*

Example 10.8. *Recall the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_m$ defined by $\phi(n) = \overline{n}$. We claim that the kernel of ϕ is:*

$$\ker \phi = m\mathbb{Z}.$$

Proof. If $\phi(n) = \overline{n} = 0$, then $n = mq + 0 = mq$ for some $q \in \mathbb{Z}$. So, $n \in m\mathbb{Z}$. Hence, $\ker \phi \subseteq m\mathbb{Z}$.

Given $mn \in m\mathbb{Z}$, where $n \in \mathbb{Z}$, the remainder $\overline{mn}$ of the division of mn by m is clearly 0, so $\phi(mn) = 0$, which implies that $m\mathbb{Z} \subseteq \ker \phi$.

Hence, $\ker \phi = m\mathbb{Z}$. □

Claim 10.9. *Let A be a commutative ring. If $\phi : A \to B$ is a ring homomorphism, then $\ker \phi$ is an ideal of A.*

Proof.

1. Since ϕ is a homomorphism, we have $\phi(0) = 0$. Hence, $0 \in \ker \phi$.
2. If $a, b \in \ker \phi$, then $\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0$. Hence, $a + b \in \ker \phi$.
3. Given any $a \in \ker \phi$, for all $r \in R$ we have $\phi(ar) = \phi(a)\phi(r) = 0 \cdot \phi(r) = 0$. Hence, $ar \in \ker \phi$ for all $r \in R$.

□

Remark.

The claim still holds if we remove the requirement that A be commutative, and "ideal" is defined using the more general definition mentioned earlier.

Claim 10.10. *A nonzero commutative ring R is a field if and only if its only ideals are $\{0\}$ and R.*

Proof. Suppose a nonzero commutative ring R is a field. If an ideal I of R is nonzero, it contains at least one nonzero element a of R.

Since R is a field, a has a multiplicative inverse a^{-1} in R. Since I is an ideal, and $a \in I$, we have $1 = a^{-1}a \in I$.

So, I is an ideal which contains 1, hence it must be the whole field R.

Conversely, let R be a nonzero commutative ring whose only ideals are $\{0\}$ and R.

Given any nonzero element $a \in R$, the principal ideal $(a) := \{ar : r \in R\}$ generated by a is nonzero because it contains $a \neq 0$.

Hence, by hypothesis the ideal (a) is necessarily the whole ring R. In particular, the element 1 lies in (a), which means that there is an $r \in R$ such that $ar = 1$. This shows that any nonzero element of R is a unit. Hence, R is a field. □

Claim 10.11. *Let k be a field, and R a nonzero ring. Any ring homomorphism $\phi : k \to R$ is necessarily one-to-one.*

Proof. Since R is not a zero ring, it contains $1 \neq 0$. So, $\phi(1) = 1 \neq 0$, which implies that $\ker \phi$ is a proper ideal of k. Since k is a field, we have $\ker \phi = \{0\}$. It now follows from a previous claim that ϕ is one-to-one. □

Example 10.12. *For any natural number $m > 1$, there can be no ring homomorphisms from $\mathbb{Q}$ to $\mathbb{Z}_m$.*

The reason is as follows:

By the previous claim, any ring homomorphism from the field $\mathbb{Q}$ to $\mathbb{Z}_m$ must be one-to-one, but there can be no one-to-one map from the infinite set $\mathbb{Q}$ to the finite set $\mathbb{Z}_m$.

10.1.1 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**

10.2 Principal Ideal Domains

For a fixed finite set of elements $a_1, a_2, \ldots, a_n$ in a commutative ring R, let $(a_1, a_2, \ldots, a_n)$ denote the subset:

$$\{r_1a_1 + r_2a_2 + \cdots + r_na_n : r_i \in R\}.$$

Claim 10.13. *The set $I = (a_1, a_2, \ldots, a_n)$ is an ideal of R.*

Proof.
1. $0 = 0 \cdot a_1 + 0 \cdot a_2 + \cdots + 0 \cdot a_n \in I$.
2. For $\sum_i r_ia_i$ and $\sum_i r'_ia_i$ in I, we have $\sum_i r_ia_i + \sum_i r'_ia_i = \sum_i (r_i + r'_i)a_i \in I$.
3. Given any $\sum_i r_ia_i \in I$, for any $r \in R$ we have $r \sum_i r_ia_i = \sum_i (rr_i)a_i \in I$.

□

We call $(a_1, a_2, \ldots, a_n)$ the ideal **generated** by $a_1, a_2, \ldots, a_n$. An ideal $(a) = \{ar : r \in R\}$ generated by one element $a \in R$ is called a **principal ideal** .

Note that $R = (1)$ and $\{0\} = (0)$ are both principal ideals.

Claim 10.14. *Given a, b in a commutative ring R. If $b = au$ for some unit $u \in R$, then $(a) = (b)$.*

If R is an integral domain and $(a) = (b)$, then $b = au$ for some unit $u \in R$.

Proof. We leave the first part of the claim as an exercise.

We now prove the second part. Suppose $(a) = (b)$. If $b = 0$, then a is necessarily zero. So, $b = 0 = 0 \cdot 1 = a \cdot 1$, and we are done.

Now suppose $b \neq 0$. The condition $(a) = (b)$ implies that there exist $u, v \in R$ such that $b = au$ and $a = bv$.

Putting the two together, we have:

$$b = buv,$$

which implies that $b(1 - uv) = 0$.

Since R is by assumption an integral domain, and $b \neq 0$, we have $1 - uv = 0$, which implies that $uv = 1$. This shows that u is unit. □

Definition 10.15. *If R is an integral domain in which every ideal is principal, we say that R is a* **Principal Ideal Domain** *(abbrev.* **PID***).*

Theorem 10.16. *The ring $\mathbb{Z}$ is a principal ideal domain.*

Proof. Let I be an ideal of $\mathbb{Z}$. We already know that the zero ideal $\{0\} = (0)$ is principal.

So, we may assume that I contains a nonzero element a. Since $-1 \in \mathbb{Z}$ and I is an ideal, we have $-a = (-1) \cdot a \in I$. Hence, if I is nonzero, it contains at least one positive integer.

By the Least Integer Axiom, the ideal I contains a positive integer d which is smaller than all other positive elements of I. We claim that $I = (d)$.

By the division theorem, for every $a \in I$, we have $a = dq + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leq r < d$. But this implies that $r = a - dq$ lies in I, since I is an ideal.

Since $0 \leq r < d$ and d is the minimal positive integer in I, r must necessarily be zero. This implies that $a = dq$. Hence, $I \subseteq (d)$.

Conversely, since $d \in I$ and I is an ideal, we have $dr \in I$ for all $r \in \mathbb{Z}$, which implies that $(d) \subseteq I$.

Hence, $I = (d)$. In other words, I is a principal ideal generated by d. □

We claim that for any field k, the ring of polynomials $k[x]$ is also a PID.

To prove this we first establish the following theorem:

Theorem 10.17 (Division Theorem for Polynomials with Unit Leading Coefficients)**.** *Let R be a commutative ring. For all $d, f \in R[x]$, such that the leading coefficient of d is a unit in R, there exist $q, r \in R[x]$ such that:*

$$f = qd + r,$$

with $\deg r < \deg d$.

Proof. The proof is essentially the same as that of the division theorem for $\mathbb{Q}[x]$. We prove by induction:

The base case corresponds to the case where $\deg f < \deg d$; and the inductive step corresponds to showing that, for any fixed d, the claim holds for f if it holds for all f' with $\deg f' < \deg f$.

Base case: If $\deg f < \deg d$, we take $r = f$. Then, indeed $f = 0 \cdot d + r$, with $\deg r < \deg d$.

Inductive step: Let $d = \sum_{i=0}^{n} a_i x^i \in R[x]$ be fixed, where a_n is a unit in R. For any given $f = \sum_{i=0}^{m} b_i x^i \in R[x]$, $m \geq n$, suppose the claim holds for all f' with $\deg f' < \deg f$.

Let:

$$f' = f - a_n^{-1} b_m x^{m-n} d.$$

Then, $\deg f' < \deg f$, hence by hypothesis there exist $q', r' \in R[x]$, with $\deg r' < \deg d$, such that:

$$f - a_n^{-1} b_m x^{m-n} d = f' = q'd + r',$$

which implies that:

$$f = (q' + a_n^{-1} b_m x^{m-n})d + r'.$$

So, $f = qd + r'$, where $q = q' + a_n^{-1} b_m x^{m-n} \in R[x]$, and $\deg r' < \deg d$. □

Theorem 10.18. *Let k be a field. Then, $k[x]$ is a PID.*

Proof. Since k is a field, the previous claim holds for all $d, f \in k[x]$ such that $d \neq 0$.

Let I be an ideal of $k[x]$.

If $I = \{0\}$ then, it is principal, since $\{0\} = (0)$.

Suppose I is nonzero. Let d be the polynomial in I with the least degree among all nonzero polynomials in I. Since the degree of any nonzero polynomial is a nonnegative integer, such an element d exists by the Least Integer Axiom. It is clear that $(d) \subseteq I$. It remains to show that $I \subseteq (d)$.

For all $f \in I$, by the previous claim we have:

$$f = qd + r,$$

for some $q, r \in k[x]$ such that $\deg r < \deg d$.

Observe that $r = f - qd = f + (-1)qd$ lies in I. Since d is a nonzero element of I with the least degree, the element r must necessarily be zero.

In order words $f = qd$, which implies that $f \in (d)$. Hence, $I \subseteq (d)$, and we may now conclude that $I = (d)$. □

10.3 Quotient Rings

Let R be a commutative ring. Let I be an ideal of R. We define a relation $\sim$ on R as follows:

$$a \sim b, \quad \text{if } a - b \in I.$$

Notation/Terminology: If $a \sim b$, we say that a is **congruent modulo** I to b, and write:

$$a \equiv b \mod I.$$

Claim 10.19. *Congruence modulo I is an* **equivalence relation** .

Proof.

- **Reflexivity** $a - a = 0 \in I$, since I is an ideal; hence, $a \equiv a \mod I$.
- **Symmetry** If $a - b \in I$, then $b - a = -1(a - b) \in I$, since I is an ideal and $-1 \in R$. Hence, $a \equiv b \mod I$ implies that $b \equiv a \mod I$.
- **Transitivity** If $a - b \in I$ and $b - c \in I$, then $a - c = a + (-b + b) - c = (a - b) + (b - c) \in I$, since I, being an ideal, is closed under addition. Hence, $a \equiv b, b \equiv c \mod I$ implies that $a \equiv c \mod I$.

□

Let R/I be the set of equivalence classes of R with respect to the relation $\sim$. Each element of R/I has the form:

$$\overline{r} = r + I = \{r + a : a \in I\}, \quad r \in R.$$

Terminology.
We call $\overline{r}$ the **residue** of r in R/I.
Note that if $r \in I$, then $\overline{r} = \overline{0}$, since $r - 0 = r \in I$.
Observe that: for all $r, r' \in R$, and $a, a' \in I$,

$$(r + a) + (r' + a') = (r + r') + (a + a') \in (r + r') + I = \overline{r + r'},$$

$$(r + a) \cdot (r' + a') = rr' + ra' + r'a + aa' \in rr' + I = \overline{rr'}.$$

Hence, we may define binary operations $+, \cdot$ on R/I as follows:

$$\overline{r} + \overline{r'} = \overline{r + r'},$$
$$\overline{r} \cdot \overline{r'} = \overline{rr'},$$

for all $\overline{r}, \overline{r'} \in R/I$.

Claim 10.20. *The set R/I, equipped with the addition $+$ and multiplication $\cdot$ defined above, is a commutative ring.*

Proof. We note here only that the additive identity element of R/I is $\overline{0} = 0 + I$, the multiplicative identity element of R/I is $\overline{1} = 1 + I$, and that $-\overline{r} = \overline{-r}$ for all $r \in R$.

We leave the rest of the proof (additive and multiplicative associativity, commutativity, distributativity) as an **Exercise.** □

Claim 10.21. *The map $\pi : R \to R/I$, defined by*

$$\pi(r) = \overline{r}, \quad \forall r \in R.$$

is a surjective ring homomorphism with kernel $\ker \pi = I$.

Proof. **Exercise.** □

Let m be a natural number. The set:

$$m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$$

is an ideal of $\mathbb{Z}$.

Claim 10.22. *The quotient ring $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to $\mathbb{Z}_m$.*

Proof. For $r \in \mathbb{Z}$, let r_m denote the remainder of the division of r by m.

Exercise: We have $\overline{r} = \overline{r_m}$ in $\mathbb{Z}/m\mathbb{Z}$, where $\bar{r}$ is the residue of r in $\mathbb{Z}/m\mathbb{Z}$.

Define a map $\phi : \mathbb{Z}_m \longrightarrow \mathbb{Z}/m\mathbb{Z}$ as follows:

$$\phi(r) = \bar{r}, \quad \forall\, r \in \mathbb{Z}_m.$$

We claim that ϕ is a homomorphism:

- $\phi(1) = \overline{1} = 1_{\mathbb{Z}/m\mathbb{Z}}$.
- $$\phi(r +_{\mathbb{Z}_m} r') = \overline{r +_{\mathbb{Z}_m} r'} = \overline{(r +_{\mathbb{Z}} r')_m} \\ = \overline{r +_{\mathbb{Z}} r'} = \overline{r} + \overline{r'} = \phi(r) + \phi(r')$$
- $$\phi(r \cdot_{\mathbb{Z}_m} r') = \overline{r \cdot_{\mathbb{Z}_m} r'} = \overline{(r \cdot_{\mathbb{Z}} r')_m} \\ = \overline{r \cdot_{\mathbb{Z}} r'} = \overline{r} \cdot \overline{r'} = \phi(r) \cdot \phi(r')$$

Hence, ϕ is a homomorphism.

Next, we show that ϕ is bijective:

For all $\bar{r} \in \mathbb{Z}/m\mathbb{Z}$, we have $\phi(r_m) = \overline{r_m} = \bar{r}$. Hence, ϕ is onto.

Suppose r is an element in $\mathbb{Z}_m$ such that $\phi(r) = \bar{r} = 0$ in $\mathbb{Z}/m\mathbb{Z}$. By definition, this means that $r \in m\mathbb{Z}$, or equivalently, that $m|r$. Since $0 \leq r < m$, we must have $r = 0$. Hence, $\ker \phi = \{0\}$. It now follows from Claim 10.4 that ϕ is one-to one.

We conclude that $\phi : \mathbb{Z}_m \longrightarrow \mathbb{Z}/m\mathbb{Z}$ is an isomorphism. □

Claim 10.23. *Let $\phi : R \longrightarrow R'$ be a ring homomorphism. Then, the image of ϕ:*

$$\operatorname{im} \phi = \{r' \in R' : r' = \phi(r) \text{ for some } r \in R\}$$

is a ring under the addition and multiplication operations of R'. (In fact, it is a subring of R'.)

Proof. **Exercise.** □

Theorem 10.24 (First Isomorphism Theorem)**.** *Let R be a commutative ring. Let $\phi : R \longrightarrow R'$ be a ring homomorphism. Then:*

$$R/\ker \phi \cong \operatorname{im} \phi,$$

(i.e. $R/\ker \phi$ is isomorphic to $\operatorname{im} \phi$.)

Proof. We define a map $\overline{\phi} : R/\ker \phi \longrightarrow \operatorname{im} \phi$ as follows:

$$\overline{\phi}(\bar{r}) = \phi(r), \quad \forall\, r \in R,$$

where $\bar{r}$ is the residue of r in $R/\ker \phi$.

We first need to check that ϕ is well-defined. Suppose $\bar{r} = \overline{r'}$, then $r' - r \in \ker \phi$. We have:

$$\phi(r') - \phi(r) = \phi(r' - r) = 0.$$

Hence, $\phi(r') = \phi(r)$. So, $\overline{\phi}$ is well-defined.

Next, we show that $\overline{\phi}$ is a homomorphism:

- $\overline{\phi}(\bar{1}) = \phi(1) = 1$;
- $\overline{\phi}(\bar{a} + \bar{b}) = \overline{\phi}(\overline{a + b}) = \phi(a + b) = \phi(a) + \phi(b) = \overline{\phi}(\bar{a}) + \overline{\phi}(\bar{b})$;
- $\overline{\phi}(\bar{a} \cdot \bar{b}) = \overline{\phi}(\overline{ab}) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(\bar{a})\overline{\phi}(\bar{b})$.

Finally, we show that $\overline{\phi}$ is a bijection, i.e. one-to-one and onto.

For any $r' \in \operatorname{im}\phi$, there exists $r \in R$ such that $\phi(r) = r'$. Since $\overline{\phi}(\overline{r}) = \phi(r) = r'$, the map $\overline{\phi}$ is onto.

Let r be an element in R such that $\overline{\phi}(\overline{r}) = \phi(r) = 0$. We have $r \in \ker\phi$, which implies that $\overline{r} = 0$ in $R/\ker\phi$. Hence, $\ker\overline{\phi} = \{0\}$, and it follows from Claim 10.4 that $\overline{\phi}$ is one-to-one. □

Corollary 10.25. *If a ring homomorphism $\phi : R \longrightarrow R'$ is surjective, then:*

$$R' \cong R/\ker\phi$$

MATH 2070A Week 11

Quotient Rings, Polynomials over a Field

11.1 Quotient Rings - continued

Example 11.1. *Let m be a natural number. Consider the map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ defined by:*

$$\phi(n) = n_m, \quad \forall\, n \in \mathbb{Z},$$

where n_m is the remainder of the division of n by m.

Exercise: *ϕ is a homomorphism.*

It is clear that ϕ is surjective, and that $\ker \phi = m\mathbb{Z}$. So, it follows from the First Isomorphism Theorem that:

$$\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}.$$

Definition 11.2 (Gaussian Integers)**.** *Let:*

$$\mathbb{Z}[i] = \{z \in \mathbb{C} : z = a + bi \text{ for some } a, b \in \mathbb{Z}\},$$

where $i = \sqrt{-1}$.

Exercise 11.3. *Show that the set $\mathbb{Z}[i]$ is a ring under the usual addition $+$ and multiplication $\times$ operations on $\mathbb{C}$.*

Moreover, we have $0_{\mathbb{Z}[i]} = 0$, $1_{\mathbb{Z}[i]} = 1$, and:

$$-(a + bi) = (-a) + (-b)i$$

for any $a, b \in \mathbb{Z}$.

Example 11.4. *The ring $\mathbb{Z}[i]/(1 + 3i)$ is isomorphic to $\mathbb{Z}/10\mathbb{Z}$.*

Proof. Define a map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}[i]/(1+3i)$ as follows:

$$\phi(n) = \overline{n}, \quad \forall\, n \in \mathbb{Z},$$

where $\overline{n}$ is the residue of $n \in \mathbb{Z}[i]$ modulo $(1+3i)$.

It is clear that ϕ is a homomorphism (**Exercise**).

Observe that in $\mathbb{Z}[i]$, we have:

$$1 + 3i \equiv 0 \mod (1+3i),$$

which implies that:

$$\begin{aligned} 1 &\equiv -3i \mod (1+3i) \\ i \cdot 1 &\equiv i \cdot (-3i) \mod (1+3i) \\ i &\equiv 3 \mod (1+3i). \end{aligned}$$

Hence, for all $a, b \in \mathbb{Z}$,

$$\overline{a+bi} = \overline{a+3b} = \phi(a+3b)$$

in $\mathbb{Z}[i]/(1+3i)$. Hence, ϕ is surjective.

Suppose n is an element of $\mathbb{Z}$ such that $\phi(n) = \overline{n} = 0$. Then, by the definition of the quotient ring we have:

$$n \in (1+3i).$$

This means that there exist $a, b \in \mathbb{Z}$ such that:

$$n = (a+bi)(1+3i) = (a-3b) + (3a+b)i,$$

which implies that $3a + b = 0$, or equivalently, $b = -3a$. Hence:

$$n = a - 3b = a - 3(-3a) = 10a,$$

which implies that $\ker \phi \subseteq 10\mathbb{Z}$. Conversely, for all $m \in \mathbb{Z}$, we have:

$$\phi(10m) = \overline{10m} = \overline{(1+3i)(1-3i)m} = 0$$

in $\mathbb{Z}[i]/(1+3i)$.

This shows that $10\mathbb{Z} \subseteq \ker \phi$. Hence, $\ker \phi = 10\mathbb{Z}$.

It now follows from the First Isomorphism Theorem that:

$$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}[i]/(1+3i).$$

□

11.2 Polynomials over a Field

Let k be a field. For $f \in k[x]$ and $a \in k$, let:

$$f(a) = \phi_a(f),$$

where ϕ_a is the **evaluation homomorphism** defined in Example 9.5. That is:

$$\phi_a\left(\sum_{i=0}^{n} c_i x^i\right) = \sum_{i=0}^{n} c_i a^i.$$

Definition 11.5. *Let $f = \sum_{i=0}^{n} c_i x^i$ be a polynomial in $k[x]$. An element $a \in k$ is a* **root** *of f if:*

$$f(a) = 0$$

in k.

Lemma 11.6. *For all $f \in k[x]$, $a \in k$, there exists $q \in k[x]$ such that:*

$$f = q(x - a) + f(a)$$

Proof. By the Division Theorem for Polynomials with Unit Leading Coefficients, there exist $q, r \in k[x]$ such that:

$$f = q(x - a) + r, \quad \deg r < \deg(x - a) = 1.$$

This implies that r is a constant polynomial.

Applying the evaluation homomorphism ϕ_a to both sides of the above equation, we have:

$$\begin{aligned} f(a) &= \phi_a(q(x - a) + r) \\ &= \phi_a(q) \cdot \phi_a(x - a) + \phi_a(r) \\ &= q(a)(a - a) + r \\ &= r. \end{aligned}$$

□

Claim 11.7 (Root Theorem)**.** *Let k be a field, f a polynomial in $k[x]$. Then, $a \in k$ is a root of f if and only if $(x - a)$ divides f in $k[x]$.*

Proof. If $a \in k$ is a root of f, then by the previous lemma there exists $q \in k[x]$ such that:

$$f = q(x - a) + \underbrace{f(a)}_{=0} = q(x - a),$$

so $(x - a)$ divides f in $k[x]$.

Conversely, if $f = q(x - a)$ for some $q \in k[x]$, then $f(a) = q(a)(a - a) = 0$. Hence, a is a root of f. □

Theorem 11.8. *Let k be a field, f a nonzero polynomial in $k[x]$.*

1. *If f has degree n, then it has at most n roots in k.*
2. *If f has degree $n > 0$ and $a_1, a_2, \ldots, a_n \in k$ are distinct roots of f, then:*

$$f = c \cdot \Pi_{i=1}^{n}(x - a_i) := c(x - a_1)(x - a_2) \cdots (x - a_n)$$

for some $c \in k$.

Proof. 1. We prove Part 1 of the claim by induction. If f has degree 0, then f is a nonzero constant, which implies that it has no roots. So, in this case the claim holds.

Let f be a polynomial with degree $n > 0$. Suppose the claim holds for all nonzero polynomials with degrees strictly less than n. We want to show that the claim also holds for f. If f has no roots in k, then the claim holds for f since $0 < n$. If f has a root $a \in k$, then by the previous claim there exists $q \in k[x]$ such that:

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

For any other root $b \in k$ of f which is different from a, we have:

$$0 = f(b) = q(b)(b - a).$$

Since k is a field, it has no zero divisors; so, it follows from $b - a \neq 0$ that $q(b) = 0$. In other words, b is a root of q. Since $\deg q < n$, by the induction hypothesis q has at most $n - 1$ roots. So, f has at most $n - 1$ roots different from a. This shows that f has at most n roots.

---

2. Let f be a polynomial in $k[x]$ which has $n = \deg f$ distinct roots $a_1, a_2, \ldots, a_n \in k$.

If $n = 1$, then $f = c_0 + c_1 x$ for some $c_i \in k$, with $c_1 \neq 0$. We have:

$$0 = f(a_1) = c_0 + c_1 a_1,$$

which implies that: $c_0 = -c_1 a_1$. Hence,

$$f = -c_1 a_1 + c_1 x = c_1(x - a_1).$$

Suppose $n > 1$. Suppose for all $n' \in \mathbb{N}$, such that $1 \leq n' < n$, the claim holds for any polynomial of degree n' which has n' distinct roots in k. By the previous claim, there exists $q \in k[x]$ such that:

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

Note that $\deg q = n - 1$.

For $1 \leq i < n$, we have

$$0 = f(a_i) = q(a_i) \underbrace{(a_i - a_n)}_{\neq 0}.$$

Since k is a field, this implies that $q(a_i) = 0$ for $1 \leq i < n$. So, $a_1, a_2, \ldots, a_{n-1}$ are $n - 1$ distinct roots of q. By the induction hypothesis there exists $c \in k$ such that:

$$q = c(x - a_1)(x - a_2) \cdots (x - a_{n-1}).$$

Hence, $f = q(x - a_n) = c(x - a_1)(x - a_2) \cdots (x - a_{n-1})(x - a_n)$.

□

Corollary 11.9. *Let k be a field. Let f, g be nonzero polynomials in $k[x]$. Let $n = \max\{\deg f, \deg g\}$. If $f(a) = g(a)$ for $n + 1$ distinct $a \in k$. Then, $f = g$.*

Proof. Let $h = f - g$, then $\deg h \leq n$. By hypothesis, there are $n + 1$ distinct elements $a \in k$ such that $h(a) = f(a) - g(a) = 0$. If $h \neq 0$, then it is a nonzero polynomial with degree $\leq n$ which has $n + 1$ distinct roots, which contradicts the previous theorem. Hence, h must necessarily be the zero polynomial, which implies that $f = g$. □

Definition 11.10. *A polynomial in $k[x]$ is called a* **monic polynomial** *if its leading coefficient is* 1.

Corollary 11.11. *Let k be a field. Let f, g be nonzero polynomials in $k[x]$. There exists a unique monic polynomial $d \in k[x]$ with the following property:*

1. $(f, g) = (d)$

   Moreover, this d also satisfies the following properties:

2. *d divides both f and g, i.e., there exists $a, b \in k[x]$ such that $f = ad$, $g = bd$.*
3. *There are polynomials $p, q \in k[x]$ such that $d = pf + qg$.*
4. *If $h \in k[x]$ is a divisor of f and g, then h divides d.*

Terminology.

- The unique monic $d \in k[x]$ which satisfies property 1 is called the **Greatest Common Divisor** (*abbrev.* **GCD**) of f and g.
- We say that f and g are **relatively prime** if their GCD is 1.

Proof. 1. By Theorem 10.18 , there exists $d = \sum_{i=0}^{n} a_i x^i \in k[x]$ such that $(d) = (f, g)$. Replacing d by $a_n^{-1} d$ if necessary, we may assume that d is a monic polynomial. It remains to show that d is unique.

Suppose $(d) = (d')$, where both d and d' are monic polynomials. Then, there exist nonzero $p, q \in k[x]$ such that:

$$d' = pd, \quad d = qd'.$$

Examining the degrees of the polynomials, we have:

$$\deg d' = \deg d + \deg p,$$

and:

$$\deg d = \deg q + \deg d' = \deg p + \deg q + \deg d.$$

This implies that $\deg p + \deg q = 0$. Hence, p and q must both have degree 0; in other words, they are constant polynomials. Moreover, we have $\deg d = \deg d'$. Comparing the leading coefficients of d' and pd, we have $p = 1$. Hence, $d = d'$.

2. Clear.

3. Clear.

4. By Part 3 of the corollary, there are $p, q \in k[x]$ such that $d = pf + qg$. It is then clear that if h divides both f and g, then h must divide d.

□

Definition 11.12. *Let R be a commutative ring. A nonzero element $p \in R$ which is not a unit is said to be* **irreducible** *if $p = ab$ implies that either a or b is a unit.*

Example 11.13. *The set of irreducible elements in the ring $\mathbb{Z}$ is $\{\pm p : p$ a prime number$\}$.*

Let k be a field.

Lemma 11.14. *A polynomial $f \in k[x]$ is a unit if and only if it is a nonzero constant polynomial.*

Proof. **Exercise.** □

Claim 11.15. *A nonzero nonconstant polynomial $p \in k[x]$ is irreducible if and only if there is no $f, g \in k[x]$, with $\deg f, \deg g < \deg p$, such that $fg = p$.*

Proof. Suppose p is irreducible, and $p = fg$ for some $f, g \in k[x]$ such that $\deg f, \deg g < \deg p$. Then $p = fg$ implies that $\deg f$ and $\deg g$ are both positive. By the previous lemma, both f and g are non-units, which is a contradiction, since the irreducibility of p implies that either f or g must be a unit.

Conversely, suppose p is a nonzero non-unit in $k[x]$, which is not equal to fg for any $f, g \in k[x]$ with $\deg f, \deg g < \deg p$. Then, $p = ab$, a, $b \in k[x]$, implies that either a or b must have the same degree as p, and the other factor must be a nonzero constant, in other words a unit in $k[x]$. Hence, p is irreducible. □

Lemma 11.16 (Euclid's Lemma)**.** *Let k be a field. Let f, g be polynomials in $k[x]$. Let p be an irreducible polynomial in $k[x]$. If $p|fg$ in $k[x]$, then $p|f$ or $p|g$.*

Proof. Suppose $p \nmid f$. Then, any common divisor of p and f must have degree strictly less than $\deg p$. Since p is irreducible, this implies that any common divisor of p and f is a nonzero constant. Hence, the GCD of p and f is 1. By Corollary 11.11 , there exist $a, b \in k[x]$ such that:

$$ap + bf = 1.$$

Multiplying both sides of the above equation by g, we have:

$$apg + bfg = g.$$

Since p divides the left-hand side of the above equation, it must also divide the right-hand side, which is the polynomial g. □

Claim 11.17. *If $f, g \in k[x]$ are relatively prime, and both divide $h \in k[x]$, then $fg|h$.*

Proof. **Exercise.** □

Theorem 11.18 (Unique Factorization)**.** *Let k be a field. Every nonconstant polynomial $f \in k[x]$ may be written as:*

$$f = cp_1 \cdots p_n,$$

where c is a nonzero constant, and each p_i is a monic irreducible polynomial in $k[x]$. The factorization is unique up to the ordering of the factors.

Proof. **Exercise.** One possible approach is very similar to the proof of unique factorization for $\mathbb{Z}$. See: The Fundamental Theorem of Arithmetic . □

Exercise 11.19. *1.* **WeBWorK**

Theorem 11.20. *Let k be a field. Let p be a polynomial in $k[x]$. The following statements are equivalent:*

1. $k[x]/(p)$ *is a field.*

2. $k[x]/(p)$ *is an integral domain.*

3. p *is irreducible in* $k[x]$.

Remark. *Compare this result with Exercise 8.11 and Corollary 8.16 .*

Proof. 1. $1 \Rightarrow 2$: Clear, since every field is an integral domain.

2. $2 \Rightarrow 3$: If p is not irreducible, there exist $f, g \in k[x]$, with degrees strictly less than that of p, such that $p = fg$. Since $\deg f, \deg g < \deg p$, the polynomial p does not divide f or g in $k[x]$. Consequently, the congruence classes $\overline{f}$ and $\overline{g}$ of f and g, respectively, modulo (p) is not equal to zero in $k[x]/(p)$. On the other hand, $\overline{f} \cdot \overline{g} = \overline{fg} = \overline{p} = 0$ in $k[x]/(p)$. This implies that $k[x]/(p)$ is not an integral domain, a contradiction. Hence, p is irreducible if $k[x]/(p)$ is an integral domain.

3. $3 \Rightarrow 1$: By definition, the multiplicative identity element 1 of a field is different from the additive identity element 0. So we need to check that the congruence class of $1 \in k[x]$ in $k[x]/(p)$ is not 0. Since p is irreducible, by definition we have $\deg p > 0$. Hence, $1 \notin (p)$, for a polynomial of degree > 0 cannot divide a polynomial of degree 0 in $k[x]$. We conclude that $1 + (p) \neq 0 + (p)$ in $k[x]/(p)$.

   Next, we need to prove the existence of the multiplicative inverse of any nonzero element in $k[x]/(p)$. Given any $f \in k[x]$ whose congruence class $\overline{f}$ modulo (p) is nonzero in $k[x]/(p)$, we want to find its multiplicative inverse $\overline{f}^{-1}$. If $\overline{f} \neq 0$ in $k[x]/(p)$, then by definition $f - 0 \notin (p)$, which means that p does not divide f. Since p is irreducible, this implies that $GCD(p, f) = 1$. By Corollary 11.11 there exist $g, h \in k[x]$ such that $fg + hp = 1$. It is then clear that $\overline{g} = \overline{f}^{-1}$, since $fg - 1 = -hp$ implies that $fg - 1 \in (p)$, which by definition means that $\overline{f} \cdot \overline{g} = \overline{fg} = 1$ in $k[x]/(p)$.

□

Example 11.21. *The rings* $\mathbb{R}[x]/(x^2 + 1)$ *and* $\mathbb{C}$ *are isomorphic.*

Proof. Define a map $\phi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ as follows:

$$\phi(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} a_k i^k.$$

Exercise: ϕ is a homomorphism.

For all $a + bi$ ($a, b \in \mathbb{R}$) in $\mathbb{C}$, we have:

$$\phi(a + bx) = a + bi.$$

Hence, ϕ is surjective.

We now find $\ker \phi$. Since $\mathbb{R}[x]$ is a PID (see Definition 10.15). There exists $p \in \mathbb{R}[x]$ such that $\ker \phi = (p)$.

Observe that $\phi(x^2 + 1) = 0$. So, $x^2 + 1 \in \ker \phi$, which implies that there exists $q \in \mathbb{R}[x]$ such that $x^2 + 1 = pq$. Since $x^2 + 1$ has no real roots, neither p or q can be of degree 1.

So, one of p or q must be a nonzero constant polynomial. p cannot be a nonzero constant polynomial, for that would imply that $\ker \phi = \mathbb{R}[x]$. So, q is a constant, which implies that $p = q^{-1}(x^2 + 1)$. We conclude that $\ker \phi = (x^2 + 1)$.

It now follows from the First Isomorphism Theorem that $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. $\square$

MATH 2070A Week 12

Rational Root Theorem, Gauss's Theorem, Eisenstein's Criterion

---

12.1 Polynomials over $\mathbb{Z}$ and $\mathbb{Q}$

Theorem 12.1 (Rational Root Theorem)**.** *Let $f = a_0 + a_1x + \cdots + a_nx^n$, be a polynomial in $\mathbb{Q}[x]$, with $a_i \in \mathbb{Z}$, $a_n \neq 0$. Every rational root r of f in $\mathbb{Q}$ has the form $r = b/c$ $(b, c \in \mathbb{Z})$ where $b|a_0$ and $c|a_n$.*

Proof. Let $r = b/c$ be a rational root of f, where b, c are relatively prime integers. We have:

$$0 = \sum_{i=0}^{n} a_i(b/c)^i$$

Multiplying both sides of the above equation by c^n, we have:

$$0 = a_0c^n + a_1c^{n-1}b + a_2c^{n-2}b^2 + \cdots + a_nb^n,$$

or equivalently:

$$a_0c^n = -(a_1c^{n-1}b + a_2c^{n-2}b^2 + \cdots + a_nb^n).$$

Since b divides the right-hand side, and b and c are relatively prime, b must divide a_0.

Similarly, we have:

$$a_nb^n = -(a_0c^n + a_1c^{n-1}b + a_2c^{n-2}b^2 + \cdots + a_{n-1}cb^{n-1}).$$

Since c divides the right-hand side, and b and c are relatively prime, c must divide a_n. □

Definition 12.2. *A polynomial $f \in \mathbb{Z}[x]$ is said to be* **primitive** *if the gcd of its coefficients is* 1.

Remark. *Note that if f is monic, i.e. its leading coefficient is 1, then it is primitive.*

If d is the gcd of the coefficients of f, then $\frac{1}{d}f$ is a primitive polynomial in $\mathbb{Z}[x]$.

Lemma 12.3 (Gauss's Lemma)**.** *If $f, g \in \mathbb{Z}[x]$ are both primitive, then fg is primitive.*

Proof. Write $f = \sum_{k=0}^{m} a_k x^k$, $g = \sum_{k=0}^{n} b_k x^k$. Then, $fg = \sum_{k=0}^{m+n} c_k x^k$, where:

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

Suppose fg is not primitive. Then, there exists a prime p such that p divides c_k for $k = 0, 1, 2, \ldots, m+n$.

Since f is primitive, there exists a least $u \in \{0, 1, 2, \ldots, m\}$ such that a_u is not divisible by p.

Similarly, since g is primitive, there is a least $v \in \{0, 1, 2, \ldots, n\}$ such that b_v is not divisible by p. We have:

$$c_{u+v} = \sum_{\substack{i+j=u+v \\ (i,j)\neq(u,v)}} a_i b_j + a_u b_v,$$

hence:

$$a_u b_v = c_{u+v} - \sum_{\substack{i+j=u+v \\ i<u}} a_i b_j - \sum_{\substack{i+j=u+v \\ j<v}} a_i b_j.$$

By the minimality conditions on u and v, each term on the right-hand side of the above equation is divisible by p.

Hence, p divides $a_u b_v$, which by Euclid's Lemma implies that p divides either a_u or b_v, a contradiction. □

Lemma 12.4. *Every nonzero $f \in \mathbb{Q}[x]$ has a unique factorization:*

$$f = c(f) f_0,$$

where $c(f)$ is a positive rational number, and f_0 is a primitive polynomial in $\mathbb{Z}[x]$.

Definition 12.5. *The rational number $c(f)$ is called the* **content** *of f.*

Proof. **Existence:**

Write $f = \sum_{k=0}^{n}(a_k/b_k)x^k$, where $a_k, b_k \in \mathbb{Z}$. Let $B = b_0 b_1 \cdots b_n$. Then, $g := Bf$ is a polynomial in $\mathbb{Z}[x]$. Let d be the gcd of the coefficients of g. Let $D = \pm d$, with the sign chosen such that $D/B > 0$. Observe that $f = c(f)f_0$, where

$$c(f) = D/B,$$

and

$$f_0 := \frac{B}{D}f = \frac{1}{D}g$$

is a primitive polynomial in $\mathbb{Z}[x]$.

Uniqueness:

Suppose $f = ef_1$ for some positive $e \in \mathbb{Q}$ and primitive $f_1 \in \mathbb{Z}[x]$. We have:

$$ef_1 = c(f)f_0.$$

Writing $e/c(f) = u/v$ where u, v are relatively prime positive integers, we have:

$$uf_1 = vf_0.$$

Since $gcd(u, v) = 1$, by Euclid's Lemma the above equation implies that v divides each coefficient of f_1, and u divides each coefficient of f_0. Since f_0 and f_1 are primitive, we conclude that $u = v = 1$. Hence, $e = c(f)$, and $f_1 = f_0$. □

Corollary 12.6. *For $f \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, we have $c(f) \in \mathbb{Z}$.*

Proof. Let d be the gcd of the coefficients of f. Then, $(1/d)f$ is a primitive polynomial, and

$$f = d\left(\frac{1}{d}f\right)$$

is a factorization of f into a product of a positive rational number and a primitive polynomial in $\mathbb{Z}[x]$. Hence, by uniqueness of $c(f)$ and f_0, we have $c(f) = d \in \mathbb{Z}$. □

Corollary 12.7. *Let f, g, h be nonzero polynomials in $\mathbb{Q}[x]$ such that $f = gh$. Then, $f_0 = g_0 h_0$ and $c(f) = c(g)c(h)$.*

Proof. The condition $f = gh$ implies that:

$$c(f)f_0 = c(g)c(h)g_0 h_0,$$

where f_0, g_0, h_0 are primitive polynomials and $c(f), c(g), c(h)$ are positive rational numbers. By a previous result $g_0 h_0$ is primitive. It now follows from the uniqueness of $c(f)$ and f_0 that $f_0 = g_0 h_0$ and $c(f) = c(g)c(h)$. □

Theorem 12.8 (Gauss's Theorem)**.** *Let f be a nonzero polynomial in $\mathbb{Z}[x]$. If $f = GH$ for some $G, H \in \mathbb{Q}[x]$, then $f = gh$ for some $g, h \in \mathbb{Z}[x]$, where $\deg g = \deg G$, $\deg h = \deg H$.*

Consequently, if f cannot be factored into a product of polynomials of smaller degrees in $\mathbb{Z}[x]$, then it is irreducible as a polynomial in $\mathbb{Q}[x]$.

Proof. Suppose $f = GH$ for some G, H in $\mathbb{Q}[x]$. Then $f = c(f)f_0 = c(G)c(H)G_0H_0$, where G_0, H_0 are primitive polynomials in $\mathbb{Z}[x]$, and $c(G)c(H) = c(f)$ by the uniqueness of the content of a polynomial.

Moreover, since $f \in \mathbb{Z}[x]$, its content $c(f)$ lies in $\mathbb{Z}$. Hence, $g = c(f)G_0$ and $h = H_0$ are polynomials in $\mathbb{Z}[x]$, with $\deg g = \deg G$, $\deg h = \deg H$, such that $f = gh$. □

Let p be a prime. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$. It is a field, since p is prime. For $a \in \mathbb{Z}$, let $\overline{a}$ denote the residue of a in $\mathbb{F}_p$.

Exercise: We have $\overline{a} = \overline{a_p}$, where a_p is the remainder of the division of a by p.

Theorem 12.9. *Let $f = \sum_{k=0}^{n} a_k x^k$ be a polynomial in $\mathbb{Z}[x]$ such that $p \nmid a_n$ (in particular, $a_n \neq 0$). If $\overline{f} := \sum_{k=0}^{n} \overline{a_k} x^k$ is irreducible in $\mathbb{F}_p[x]$, then f is irreducible in $\mathbb{Q}[x]$.*

Proof. Suppose $\overline{f}$ is irreducible in $\mathbb{F}_p[x]$, but f is not irreducible in $\mathbb{Q}[x]$. By Gauss's theorem, there exist $g, h \in \mathbb{Z}[x]$ such that $\deg g, \deg h < \deg f$ and $f = gh$.

Since by assumption $p \nmid a_n$, we have $\deg \overline{f} = \deg f$.

Moreover, $\overline{gh} = \overline{g} \cdot \overline{h}$ (**Exercise**).

Hence, $\overline{f} = \overline{gh} = \overline{g} \cdot \overline{h}$, where $\deg \overline{g}, \deg \overline{h} < \deg \overline{f}$. This contradicts the irreducibility of $\overline{f}$ in $\mathbb{F}_p[x]$.

Hence, f is irreducible in $\mathbb{Q}[x]$ if $\overline{f}$ is irreducible in $\mathbb{F}_p[x]$. □

Example 12.10. *The polynomial $f(x) = x^4 - 5x^3 + 2x + 3 \in \mathbb{Q}[x]$ is irreducible.*

Proof. Consider $\overline{f} = x^4 - \overline{5}x^3 + \overline{2}x + \overline{3} = x^4 + x^3 + 1$ in $\mathbb{F}_2[x]$. If we can show that $\overline{f}$ is irreducible, then by the previous theorem we can conclude that f is irreducible.

Since $\mathbb{F}_2 = \{0, 1\}$ and $\overline{f}(0) = \overline{f}(1) = 1 \neq 0$, we know right away that $\overline{f}$ has no linear factors. So, if $\overline{f}$ is not irreducible, it must be a product of two quadratic factors:

$$\overline{f} = (ax^2 + bx + c)(dx^2 + ex + g), \quad a, b, c, d, e, g \in \mathbb{F}_2.$$

Note that by assumption a, d are nonzero elements of $\mathbb{F}_2$, so $a = d = 1$. This implies that, in particular:

$$1 = \overline{f}(0) = cg$$
$$1 = \overline{f}(1) = (1 + b + c)(1 + e + g)$$

The first equation implies that $c = g = 1$. The second equation then implies that $1 = (2 + b)(2 + e) = be$. Hence, $b = e = 1$.

We have:

$$x^4 + x^3 + 1 = (x^2 + x + 1)(x^2 + x + 1)$$
$$= x^4 + 2x^3 + 3x^2 + 2x + 1 = x^4 + x^2 + 1,$$

a contradiction.

Hence, $\overline{f}$ is irreducible in $\mathbb{F}_2[x]$, which implies that f is irreducible in $\mathbb{Q}[x]$. □

Theorem 12.11 (Eisenstein's Criterion)**.** *Let $f = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial in $\mathbb{Z}[x]$. If there exists a prime p such that $p | a_i$ for $0 \leq i < n$, but $p \nmid a_n$ and $p^2 \nmid a_0$, then f is irreducible in $\mathbb{Q}[x]$.*

Proof. We prove by contradiction. Suppose f is not irreducible in $\mathbb{Q}[x]$. Then, by Gauss's Theorem, there exists $g = \sum_{k=0}^{l} b_k x^k$, $h = \sum_{k=0}^{n-l} c_k x^k \in \mathbb{Z}[x]$, with $\deg g, \deg h < \deg f$, such that $f = gh$.

Consider the image of these polynomials in $\mathbb{F}_p[x]$. By assumption, we have:

$$\overline{a_n} x^n = \overline{f} = \overline{g}\overline{h}.$$

This implies that $\overline{g}$ and $\overline{h}$ are divisors of $\overline{a_n} x^n$. Since $\mathbb{F}_p$ is a field, unique factorization holds for $\mathbb{F}_p[x]$. Hence, we must have:

$$\overline{g} = \overline{b_u} x^u, \quad \overline{h} = \overline{c_{n-u}} x^{n-u},$$

for some $u \in \{0, 1, 2, \ldots, l\}$.

If $u < l$, then $n - u > n - l \geq \deg \overline{h}$, which cannot hold.

So, we conclude that $\overline{g} = \overline{b_l} x^l$, $\overline{h} = \overline{c_{n-l}} x^{n-l}$.

In particular, $\overline{b_0} = \overline{c_0} = 0$ in $\mathbb{F}_p$, which implies that p divides both b_0 and c_0. Since $a_0 = b_0 c_0$, we have $p^2 | a_0$, a contradiction. □

Example 12.12. *The polynomial $x^5 + 3x^4 - 6x^3 + 12x + 3$ is irreducible in $\mathbb{Q}[x]$.*

MATH 2070A Week 13

Field Extensions, Finite Fields

13.1 Field Extensions

Definition 13.1. *Let R be a ring. A subset S of R is said to be a* **subring** *of R if it is a ring under the addition $+_R$ and multiplication $\times_R$ associated with R, and its additive and multiplicative identity elements 0, 1 are those of R.*

Remark. *To show that a subset S of a ring R is a subring, it suffices to show that:*

- *S contains the additive and multiplicative identity elements of R.*
- *S is "closed under addition": $a +_R b \in S$ for all $a, b \in S$.*
- *S is "closed under multiplication": $a \times_R b \in S$ for all $a, b \in S$.*
- *S is closed under additive inverse: For all $a \in S$, the additive inverse $-a$ of a in R belongs to S.*

Definition 13.2. *A* **subfield** *k of a field K is a subring of K which is a field.*

In particular, for each nonzero element $r \in k \subseteq K$. The multiplicative inverse of r in K lies k.

Definition 13.3. *Let K be a field and k a subfield. Let α be an element of K. We define $k(\alpha)$ to be the smallest subfield of K containing k and α. In other words, if F is a subfield of K which contains k and α, then $F \supseteq k(\alpha)$. We say that $k(\alpha)$ is obtained from k by* **adjoining** *α.*

Theorem 13.4. *Let k be a subfield of a field K. Let α be an element of K.*

1. *If α is a root of a nonzero polynomial $f \in k[x]$ (viewed as a polynomial in $K[x]$ with coefficients in k), then α is a root of an irreducible polynomial $p \in k[x]$, such that $p|f$ in $k[x]$.*

2. *Let p be an irreducible polynomial in $k[x]$ of which α is a root. Then, the map $\phi : k[x]/(p) \longrightarrow K$, defined by:*

$$\phi\left(\sum_{j=0}^{n} c_j x^j + (p)\right) = \sum_{j=0}^{n} c_j \alpha^j,$$

   is a well-defined one-to-one ring homomorphism with $\operatorname{im}\phi = k(\alpha)$. (Here, $\sum_{j=0}^{n} c_j x^j + (p)$ is the congruence class of $\sum_{j=0}^{n} c_j x^j \in k[x]$ modulo (p).) Hence,

$$k[x]/(p) \cong k(\alpha).$$

3. *If $\alpha, \beta \in K$ are both roots of an irreducible polynomial p in $k[x]$, then there exists a ring isomorphism $\sigma : k(\alpha) \longrightarrow k(\beta)$, with $\sigma(\alpha) = \beta$ and $\sigma(s) = s$, for all $s \in k$.*

4. *Let p be an irreducible polynomial in $k[x]$ of which α is a root. Then, each element in $k(\alpha)$ has a unique expression of the form:*

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1},$$

   where $c_i \in k$, and $n = \deg p$.

Remark. *Suppose p is an irreducible polynomial in $k[x]$ of which $\alpha \in K$ is a root. Part 4 of the theorem essentially says that $k(\alpha)$ is a vectors space of dimension $\deg p$ over k, with basis:*

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}.$$

Example 13.5. *Consider $k = \mathbb{Q}$ as a subfield of $K = \mathbb{R}$. The element $\alpha \in \sqrt[3]{2} \in \mathbb{R}$ is a root of the the polynomial $p = x^3 - 2 \in \mathbb{Q}[x]$, which is irreducible in $\mathbb{Q}[x]$ by the Eisenstein's Criterion for the prime 2.*

The theorem applied to this case says that $\mathbb{Q}(\alpha)$, i.e. the smallest subfield of $\mathbb{R}$ containing $\mathbb{Q}$ and α, is equal to the set:

$$\{c_0 + c_1\alpha + c_2\alpha^2 : c_i \in \mathbb{Q}\}$$

The addition and multiplication operations in $\mathbb{Q}(\alpha)$ are those associated with $\mathbb{R}$, in other words:

$$(c_0 + c_1\alpha + c_2\alpha^2) + (b_0 + b_1\alpha + b_2\alpha^2) \\ = (c_0 + b_0) + (c_1 + b_1)\alpha + (c_2 + b_2)\alpha^2,$$

$$
\begin{aligned}
(c_0 + c_1\alpha + c_2\alpha^2) \cdot (b_0 + b_1\alpha + b_2\alpha^2) & \\
&= c_0b_0 + c_0b_1\alpha + c_0b_2\alpha^2 + c_1b_0\alpha + c_1b_1\alpha^2 \\
&\quad + c_1b_2\alpha^3 + c_2b_0\alpha^2 + c_2b_1\alpha^3 + c_2b_2\alpha^4 \\
&= (c_0b_0 + 2c_1b_2 + 2c_2b_1) + (c_0b_1 + c_1b_0 + 2c_2b_2)\alpha \\
&\quad + (c_0b_2 + c_1b_1 + c_2b_0)\alpha^2
\end{aligned}
$$

Exercise 13.6. *Given a nonzero $\gamma = c_0 + c_1\alpha + c_2\alpha^2 \in \mathbb{Q}(\alpha)$, $c_i \in \mathbb{Q}$, find $b_0, b_1, b_2 \in \mathbb{Q}$ such that $b_0 + b_1\alpha + b_2\alpha^2$ is the multiplicative inverse of γ in $\mathbb{Q}(\alpha)$.*

Proof. (of Theorem 13.4)

1. Define a map $\psi : k[x] \longrightarrow K$ as follows:

$$\psi\left(\sum c_j x^j\right) = \sum c_j \alpha^j.$$

   Exercise: ψ is a ring homomorphism.

   By assumption, f lies in $\ker\psi$. Since k is a field, the ring $k[x]$ is a PID. So, there exists $p \in k[x]$ such that $\ker\psi = (p)$. Hence, $p|f$ in $k[x]$.

   By the First Isomorphism Theorem, $\operatorname{im}\psi$ is a subring of K which is isomorphic to $k[x]/(p)$. In particular, $\operatorname{im}\psi$ is an integral domain because K has no zero divisors. Hence, by Theorem 11.20 , the polynomial p is an irreducible in $k[x]$.

   Since $p \in (p) = \ker\psi$, we have $0 = \psi(p) = p(\alpha)$. Hence, α is a root of p.

2. If $f+(p) = g+(p)$ in $k[x]/(p)$, then $g-f \in (p)$, or equivalently: $g = f+pq$ for some $q \in k[x]$.

   Hence, $\phi(g + (p)) = f(\alpha) + p(\alpha)q(\alpha) = f(\alpha) = \phi(f + (p))$.

   This shows that ϕ is a well-defined map. We leave it as an exercise to show that ϕ is a one-to-one ring homomorphism.

   We now show that $\operatorname{im}\phi = k(\alpha)$. By the First Isomorphism Theorem, $\operatorname{im}\phi$ is isomorphic to $k[x]/(p)$, which is a field since p is irreducible. Moreover, $\alpha = \phi(x + (p))$ lies in $\operatorname{im}\phi$. Hence, $\operatorname{im}\phi$ is a subfield of K containing α.

   Since each element in $\operatorname{im}\phi$ has the form $\sum_{j=0}^{n} c_j\alpha^j$, where $c_j \in k$, and fields are closed under addition and multiplication, any subfield of K which contains k and α must contain $\operatorname{im}\phi$. This shows that $\operatorname{im}\phi$ is the smallest subfield of K containing k and α. Hence, $k[x]/(p) \cong \operatorname{im}\phi = k(\alpha)$.

3. Define $\phi' : k[x]/(p) \longrightarrow k(\beta)$ as follows:

$$\phi'\left(\sum c_j x^j + (p)\right) = \sum c_j \beta^j.$$

By the same reasoning applied to ϕ before, the map ϕ' is a well-defined ring isomorphism, with:

$$\phi'(x + (p)) = \beta, \quad \phi'(s + (p)) = s \text{ for all } s \in k.$$

It is then easy to see that the map $\sigma := \phi' \circ \phi^{-1} : k(\alpha) \longrightarrow k(\beta)$ is the desired isomorphism between $k(\alpha)$ and $k(\beta)$.

4. Since ϕ in Part 2 is an isomorphism onto $\operatorname{im}\phi = k(\alpha)$, we know that each element $\gamma \in k(\alpha)$ is equal to $\phi(f + (p)) = f(\alpha) := \sum c_j \alpha^j$ for some $f = \sum c_j x^j \in k[x]$.

By the division theorem for $k[x]$. There exist $m, r \in k[x]$ such that $f = mp + r$, with $\deg r < \deg p = n$. In particular, $f + (p) = r + (p)$ in $k[x]/(p)$.

Write $r = \sum_{j=0}^{n-1} b_j x^j$, with $b_j = 0$ if $j > \deg r$.

We have:

$$\gamma = \phi(f + (p)) = \phi(r + (p)) = \sum_{j=0}^{n-1} b_j \alpha^j.$$

It remains to show that this expression for γ is unique. Suppose $\gamma = g(\alpha) = \sum_{j=0}^{n-1} b'_j \alpha^j$ for some $g = \sum_{j=0}^{n-1} b'_j x^j \in k[x]$.

Then, $g(\alpha) = r(\alpha) = \gamma$ implies that $\phi(g + (p)) = \phi(r + (p))$, hence:

$$(g - r) + (p) \in \ker \phi.$$

Since ϕ is one-to-one, we have $(g - r) \equiv 0$ modulo (p), which implies that $p|(g - r)$ in $k[x]$.

Since $\deg g, \deg r < \deg p$, this implies that $g - r = 0$. So, the expression $\gamma = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ is unique.

□

Terminology:

- If k is a subfield of K, we say that K is a **field extension** of k.
- Let α be an element in a field extension K of a field k. If there exists a polynomial $p \in k[x]$ of which α is a root, then α is said to be **algebraic over** k.

- If $\alpha \in K$ is algebraic over k, then there exists a unique *monic irreducible* polynomial $p \in k[x]$ of which α is a root (**Exercise**). This polynomial p is called the **minimal polynomial** of α over k.

For example, $\sqrt[3]{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$. Its minimal polynomial over $\mathbb{Q}$ is $x^3 - 2$.

Exercise 13.7. *Find the minimal polynomial of* $2 - \sqrt[3]{6} \in \mathbb{R}$ *over* $\mathbb{Q}$*, if it exists.*

Exercise 13.8. *Find the minimal polynomial of* $\sqrt[3]{5}$ *over* $\mathbb{Q}$*.*

Exercise 13.9. *Express the multiplicative inverse of* $\gamma = 2 + \sqrt[3]{5}$ *in* $\mathbb{Q}(\sqrt[3]{5})$ *in the form:*

$$\gamma^{-1} = c_0 + c_1\sqrt[3]{5} + c_2\left(\sqrt[3]{5}\right)^2,$$

where $c_i \in \mathbb{Q}$*, if possible.*

13.2 Splitting Field

Example 13.10. *Since* $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$ *is a root of* $x^3 - 2$*, the polynomial* $p = x^3 - 2$ *has a linear factor in* $\mathbb{Q}(\sqrt[3]{2})[x]$*. More precisely,*

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$$

in $\mathbb{Q}(\sqrt[3]{2})[x]$*.* **Exercise***: Is* $x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2$ *irreducible in* $\mathbb{Q}(\sqrt[3]{2})[x]$*?*

We could repeat this process and adjoin roots of $x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2$ to $\mathbb{Q}(\sqrt[3]{2})$ to further "split" the polynomial $x^3 - 2$ into a product of linear factors. That is the main idea behind the following theorem:

Theorem 13.11. *If* k *is a field, and* f *is a nonconstant polynomial in* $k[x]$*, then there exists a field extension* K *of* k*, such that* $f \in k[x] \subseteq K[x]$ *is a product of linear factors in* $K[x]$*.*

In other words, there exists a field extension K *of* k*, such that:*

$$f = c(x - \alpha_1) \cdots (x - \alpha_n),$$

for some $c, \alpha_i \in K$*.*

Proof. We prove by induction on $\deg f$.

If $\deg f = 1$, we are done.

Inductive Step: Suppose $\deg f > 1$. Suppose, for any field extension k' of k, and any polynomial $g \in k'[x]$ with $\deg g < \deg f$, there exists a field extension K of k' such that g splits into a product of linear factors in $K[x]$.

Suppose f is irreducible. Let $f(t)$ be the polynomial in $k[t]$ obtained from f by replacing the variable x with the variable t. Consider $k' := k[t]/(f(t))$. Then, k' is a field extension of k if we identify k with the subset $\{c + (f(t)) : c \in k\} \subseteq k'$, where c is considered as a constant polynomial in $k[t]$.

Observe that k' contains a root α of f, namely $\alpha = t + (f(t)) \in k[t]/(f(t))$. Hence, $f = (x - \alpha)q$ in $k'[x]$ for some polynomial $q \in k'[x]$ with $\deg q < \deg f$.

Now, by the induction hypothesis, there is an extension field K of k' such that q splits into a product of linear factors in $K[x]$. Consequently, f splits into a product of linear factors in $K[x]$.

If f is not irreducible, then $f = gh$ for some $g, h \in k[x]$, with $\deg g, \deg h < \deg f$. So, by the induction hypothesis, there is a field extension k' of k such that g is a product of linear factors in $k'[x]$.

Hence, $f = (x - \alpha_1) \cdots (x - \alpha_n)h$ in $k'[x]$. Since $\deg h < \deg f$, by the inductive hypothesis there exists a field extension K of k' such that h splits into linear factors in $K[x]$.

Hence, f is a product of linear factors in $K[x]$. □

13.3 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**

@thm If k is a field, and f is a nonconstant polynomial in $k[x]$, then there exists a field extension K of k, such that $f \in k[x] \subseteq K[x]$ is a product of linear factors in $K[x]$. @newcol In other words, there exists a field extension K of k, such that:

$$f = c(x - \alpha_1) \cdots (x - \alpha_n),$$

for some $c, \alpha_i \in K$. @endcol@end@proof@newcol We prove by induction on $\deg f$. @col If $\deg f = 1$, we are done. @colInductive Step: Suppose $\deg f > 1$. Suppose, for any field extension k' of k, and any polynomial $g \in k'[x]$ with $\deg g < \deg f$, there exists a field extension K of

k' such that g splits into a product of linear factors in $K[x]$. @col Suppose f is irreducible. Let $f(t)$ be the polynomial in $k[t]$ obtained from f by replacing the variable x with the variable t. Consider $k' := k[t]/(f(t))$. Then, k' is a field extension of k if we identify k with the subset $\{c + (f(t)) : c \in k\} \subseteq k'$, where c is considered as a constant polynomial in $k[t]$. @col Observe that k' contains a root α of f, namely $\alpha = t + (f(t)) \in k[t]/(f(t))$. Hence, $f = (x - \alpha)q$ in $k'[x]$ for some polynomial $q \in k'[x]$ with $\deg q < \deg f$. @col Now, by the induction hypothesis, there is an extension field K of k' such that q splits into a product of linear factors in $K[x]$. Consequently, f splits into a product of linear factors in $K[x]$. @col If f is not irreducible, then $f = gh$ for some $g, h \in k[x]$, with $\deg g, \deg h < \deg f$. So, by the induction hypothesis, there is a field extension k' of k such that g is a product of linear factors in $k'[x]$. @col Hence, $f = (x-\alpha_1)\cdots(x-\alpha_n)h$ in $k'[x]$. Since $\deg h < \deg f$, by the inductive hypothesis there exists a field extension K of k' such that h splits into linear factors in $K[x]$. @col Hence, f is a product of linear factors in $K[x]$. @qed@endcol@end

13.4 Finite Fields

Recall:

Definition 13.12. *Let R be a ring with additive and multiplicative identity elements 0, 1, respectively. The* **characteristic** $\operatorname{char} R$ *of R is the smallest positive integer n such that:*

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0.$$

If such an integer does not exist, we say that the ring has **characteristic zero**.

Example 13.13.

- *The ring $\mathbb{Q}$ has characteristic zero.*
- $\operatorname{char} \mathbb{Z}_6 = 6$.

Exercise 13.14. *If a ring R as finitely many elements, then it has positive (i.e. nonzero) characteristic.*

Claim 13.15. *If a field F has positive characteristic $\operatorname{char} F$, then $\operatorname{char} F$ is a prime number.*

Example 13.16. $\operatorname{char} \mathbb{F}_5 = 5$*, which is prime.*

Remark. *Note that all finite rings have positive characteristics, but there are rings with positive characteristics which have infinitely many elements, e.g. the polynomial ring $\mathbb{F}_5[x]$.*

Claim 13.17. *Let F be a finite field. Then, the number of elements of F is equal to p^n for some prime p and $n \in \mathbb{N}$.*

Proof. Since F is finite, it has finite characteristic. Since it is a field, $\operatorname{char} F$ is a prime p.

Exercise: $\mathbb{F}_p$ is isomorphic to a subfield of F.

Viewing $\mathbb{F}_p$ as a subfield of F, we see that F is a vector space over $\mathbb{F}_p$. Since the cardinality of F is finite, the dimension n of F over $\mathbb{F}_p$ must necessarily be finite.

Hence, there exist n basis elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in F, such that each element of F may be expressed uniquely as:

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n,$$

where $c_i \in \mathbb{F}_p$.

Since $\mathbb{F}_p$ has p elements, it follows that F has p^n elements. □

Claim 13.18. *Let k be a field, f a nonzero irreducible polynomial in $k[x]$, then $k[x]/(f)$ is a vector space of dimension $\deg f$ over k.*

Proof. Let $K = k[t]/(f(t))$, then K is a field extension of k which contains a root α of f, namely, $\alpha = t + (f(t))$.

It is clear that $K = k(\alpha)$, since any element in $K = k[t]/(f(t))$ has the form $\sum b_i\alpha^i$, where $b_i \in k$.

On the other hand, by Theorem 13.4, every element in $k(\alpha)$ may be expressed uniquely in the form:

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}, \quad c_i \in k,\ n = \deg f,$$

which shows that $K = k(\alpha)$ is a vector space of dimension $\deg f$ over k.

Since K is simply $k[x]/(f)$ with the variable x replaced with t, we conclude that $k[x]/(f)$ is a vector space of dimension $\deg f$ over k. □

Corollary 13.19. *If k is a finite field with $|k|$ elements, and f is an irreducible polynomial of degree n in $k[x]$, then the field $k[x]/(f)$ has $|k|^n$ elements.*

Example 13.20. *Let $p = 2$, $n = 2$. To construct a finite field with $p^n = 4$ elements. We first start with the finite field $\mathbb{F}_2$, then try to find an irreducible polynomial $f \in \mathbb{F}_2[x]$ such that $\mathbb{F}_2[x]/(f)$ has 4 elements.*

Based on our discussion so far, the degree of f should be equal to $n = 2$, since n is precisely the dimension of the desired finite field over $\mathbb{F}_2$.

Consider $f = x^2 + x + 1$. Since p is of degree 2 and has no root in $\mathbb{F}_2$, it is irreducible in $\mathbb{F}_2[x]$. Hence, $\mathbb{F}_2[x]/(x^2 + x + 1)$ is a field with 4 elements.

Theorem 13.21. *(***Galois** *) Given any prime p and $n \in \mathbb{N}$, there exists a finite field F with p^n elements.*

Proof. (Not within the scope of the course.)

Consider the polynomial:

$$f = x^{p^n} - x \in \mathbb{F}_p[x]$$

By Kronecker's theorem, there exists a field extension K of $\mathbb{F}_p$ such that f splits into a product of linear factors in $K[x]$. Let:

$$F = \{\alpha \in K : f(\alpha) = 0\}.$$

Exercise 13.22. *Let $g = (x - a_1)(x - a_2) \cdots (x - a_n)$ be a polynomial in $k[x]$, where k is a field. Show that the roots $a_1, a_2, \ldots, a_n$ are distinct if and only if $gcd(g, g') = 1$, where g' is the derivative of g.*

In this case, we have $f' = p^n x^{p^n - 1} - 1 = -1$ in $\mathbb{F}_p[x]$. Hence, $gcd(f, f') = 1$, which implies by the exercise that the roots of f are all distinct. So, f has p^n distinct roots in K, hence F has exactly p^n elements.

It remains to show that F is a field. Let $q = p^n$. By definition, an element $a \in K$ belongs to F if and only if $f(a) = a^q - a = 0$, which holds if and only if $a^q = a$. For $a, b \in F$, we have:

$$(ab)^q = a^q b^a = ab,$$

which implies that F is closed under multiplication. Since K, being a extension of $\mathbb{F}_p$, has characteristic p. we have $(a + b)^p = a^p + b^p$. Hence,

$$\begin{aligned}(a + b)^q = (a + b)^{p^n} &= ((a + b)^p)^{p^{n-1}} = (a^p + b^p)^{p^{n-1}} \\ &= (a^p + b^p)^p)^{p^{n-2}} = (a^{p^2} + b^{p^2})^{p^{n-2}} \\ &= \cdots = a^{p^n} + b^{p^n} = a + b,\end{aligned}$$

which implies that F is closed under addition.

Let $0, 1$ be the additive and multiplicative identity elements, respectively, of K. Since $0^q = 0$ and $1^q = 1$, they are also the additive and multiplicative identity elements of F.

For nonzero $a \in F$, we need to prove the existence of the additive and multiplicative inverses of a in F.

Let $-a$ be the additive inverse of a in K. Since $(-1)^q = -1$ (even if $p = 2$, since $1 = -1$ in $\mathbb{F}_2$), we have:

$$(-a)^q = (-1)^q a^q = -a,$$

so $-a \in F$. Hence, $a \in F$ has an additive inverse in F. Since $a^q = a$ in K, we have:

$$a^{q-2}a = a^{q-1} = 1$$

in K. Since $a \in F$ and F is closed under multiplication, $a^{q-2} = \underbrace{a \cdots a}_{q-2 \text{ times}}$ lies in F. So, a^{q-2} is a multiplicative inverse of a in F. $\square$