# MATH403: Introduction to Abstract Algebra

Michael Li

## Symmetry and Counting

Consider the example of coloring the 6 vertices of a hexagon, 3 black and 3 white. There are $\binom{6}{3} = 20$ possibilities

However, in reality we would count designs that can be obtained from rotation the same design

- Furthermore, designs that are equivalent under rotation are nonequivalent to other design types
- Similar concept can be extended to $D_6$

Two designs $A, B$ are **equivalent** under a group $G$ of permutations of arrangements if $\exists \phi \in G$ such that $\phi(A) = B$

- This means that the two designs are in the same orbit of $G$
- It follows that the number of nonequivalent designs under $G$ is the number of orbits of designs under $G$

### Burnside's Theorem

Few notations to mention. If $G$ is a group of permutations on a set $S$ and $i \in S$

- $\text{stab}_G(i) = \{\phi \in G \mid \phi(i) = i\}$
- $\text{orb}_G(i) = \{\phi(i) \mid \phi \in G\}$

**Fixed**: for any $G$ of permutations on set $S$ and $\phi \in G$, $\text{fix}(\phi) = \{i \in S \mid \phi(i) = i\}$. Elements fixed by $\phi$

**Burnside's Theorem**: If $G$ is a finite group of permutations on set $S$, then the number of orbits of $S$ under $G$ is $\frac{1}{|G|}\sum_{\phi \in G} |\text{fix}(\phi)|$

- Proof: let $n$ denotes the number of pairs of $(\phi, i)$ where $\phi(i) = i$. There are 2 ways to count these pairs

  $n = \sum_{\phi \in G} |\text{fix}(\phi)|$

  $n = \sum_{i \in S} |\text{stab}_G(i)|$

  From Exercise 7.43 (orbits of $S$ partition $S$), if $s, t$ are in the same orbit of $G$, then $\text{orb}_G(s) = \text{orb}_G(t)$. Thus from Orbit-Stabilizer Theorem, $|\text{stab}_G(s)| = |G|/|\text{orb}_G(s)| = |G|/|\text{orb}_G(t)| = |\text{stab}_G(t)|$

  Choosing $s \in S$ and summing over $\text{orb}_G(s)$, we get $\sum_{t \in \text{orb}_G(s)} |\text{stab}_G(t)| = |\text{orb}_G(s)||\text{stab}_G(s)| = |G|$

  Finally summing over elements of $G$, one orbit at a time, we get

$$\sum_{\phi \in G} |\text{fix}(\phi)| = \sum_{i \in S} |\text{stab}(i)| = |G| * (\text{number of orbits})$$

**Examples**:

- Hexagon vertex coloring, 3 black, 3 white, under rotation
  - Identity fix 20 designs
  - Rotation by 60 degrees fixes 0 designs
  - Rotation by 120 degrees fixes 2 designs
  - Rotation by 180 degrees fixes 0 designs
  - Rotation by 240 degrees fixes 2 designs

- Rotation by 300 degrees fixes 0 designs

  Thus from Burnside's Theorem, we have that number of orbits is $\frac{1}{6}(20+0+2+0+2+0) = 4$ number of orbits

- Hexagon vertex coloring, 3 black, 3 white, under $D_6$

  **Note**: two arrangements are equivalent if they are in the same orbit under $D_6$

  - Identity fix 20 designs
  - Rotation of order 2 (180 degrees) fixes 0 designs
  - Rotation of order 3 (120 or 240 degrees) fixes 2 designs
  - Rotation of order 6 (60 or 300 degrees) fixes 0 designs
  - Reflection across diagonal (3 of these) fixes 4 designs
  - Reflection across side bisector (3 of these) fixes 0 designs

    Thus from Burnside's Theorem, we have number of orbits is $\frac{1}{12}(1*20+1*0+2*2+2*0+3*4+3*0) = 3$ number of orbits

- 3 coloring (R, W, B) of edges of a tetrahedron

  There are $3^6 = 729$ total colorings, ignoring equivalence

  Colorings are considered equivalent under rotation so we have a group of 12 rotations and is isomorphic to $A_4$

  - Identity fixes $3^6 = 729$ designs
  - $(abc)$ (there are $4*3*2/3 = 8$ of these) fixes $3^2$ designs
  - $(ab)(cd)$ (there are $4*3*2*1/(2*2*2) = 3$ of these) fixes $3^4$ designs

  Thus from Burnside's Theorem, we have number of orbits is $\frac{1}{12}(1*3^6+8*3^2+3*3^4) = 87$ number of orbits

### Group Actions

**Group Action**: Homomorphism $\gamma$ from $G$ to sym($S$)

- image of $g$ under of $\gamma$ is denoted $\gamma_g$
- $x, y \in S$ are viewed as equivalent under action of $G$ if and only if $\gamma_g(x) = y$ for some $g \in G$
- When $\gamma$ is one to one, elements of $G$ may be regarded as permutations on $S$
- When $\gamma$ is not one to one, elements of $G$ can still be regarded as permutations on $S$, but there distinct elements $g, h \in G$ such that $\gamma_g, \gamma)h$ induce the same permutations on $S$

  $\forall x \in S, \gamma_g(x) = \gamma_h(x)$

## Intro to Rings

**Ring**: a set $R$ with 2 binary operations $(a+b, ab)$ such that $\forall a, b, c \in R$:

1. $a+b = b+a$
2. $(a+b)+c = a+(b+c)$
3. Exists an additive identity 0 such that $\forall a \in R, a+0 = a$
4. For each $a \in R$, exists an additive inverse $-a$ such that $a+(-a) = 0$
5. $a(bc) = (ab)c$
6. $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$

**UPSHOT**: ring is an Abelian group under addition with associative multiplication that distributes over addition

- **Commutative ring**: ring with commutative multiplication. Doesn't have to hold
- **Unity**: nonzero element in ring that is an identity under mulitplication. Doesn't have to exist
- **Unit**: element in $R$ with a multiplicative inverse. Doesn't have to exist

**Examples**:

- $\mathbb{Z}$ under ordinary $+, \times$ is a commutative ring with unity 1
  - Units of $\mathbb{Z}$ are $1, -1$
- $\mathbb{Z}_n$ under $+, \times \pmod n$ is a commutative ring with unity 1

  - Units are $U(n)$

- $\mathbb{Z}[x]$ polynomials under function $+, \times$ is a commutative ring with unity $f(x) = 1$
- $M_2(\mathbb{Z})$ is a noncommutative ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
- $2\mathbb{Z}$ under ordinary $+, \times$ is a commutative ring without unity
- Let $R_1, \ldots, R_n$ be rings, then $R_1 \oplus \cdots \oplus R_n = \{(a_1, \ldots, a_n) \mid a_i \in R_i\}$ is a ring under componentwise addition and multiplication called the **direct sum** of $R_1, \ldots R_n$

## Properties of Rings

**Theorem 12.1** Rules of Multiplication:

1. $a0 = 0a = 0$
   - Proof: $0 + a0 = a0 = a(0+0) = a0 + a0 \implies a0 = 0$. Similarly, $0a = 0$
2. $a(-b) = (-a)b = -(ab)$
   - Proof: $a(-b) + ab = a(-b+b) = a0 = 0$. Adding both sides by $-(ab)$ yields $a(-b) = -(ab)$. Similarly, $(-a)b = -(ab)$
3. $(-a)(-b) = ab$
   - Proof: applying 2., we get $(-a)(-b) = -((-a)b) = -(-(ab)) = ab$
4. $a(b-c) = ab - ac$ and $(b-c)a = ba - ca$
   - Proof: by distributing and applying 2., we get $a(b-c) = a(b+(-c)) = ab + a(-c) = ab - ac$

If $R$ has unity element of 1, we can claim that

5. $(-1)a = -a$

- Proof: applying 2., we get $(-1)a = -(1a) = -a$

6. $(-1)(-1) = 1$

- Proof: applying 2., we get $(-1)(-1) = -(-1) = 1$

**Theorem 12.2**: If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique

- Proof: Let $e_1, e_2$ be distinct unities of $R$. Then $e_1e_2 = e_1$ and $e_1e_2 = e_2 \implies e_1 = e_2$

  Let $b, c$ both be multiplicative inverses of $a$. Then $ab = ac = e \implies b = c$. Similar for right multiplicative inverse

**Note**: cannot always say that

- $ab = ac \implies b = c$ since multiplicative cancellation is not guaranteed
- $a^2 = a \implies a = 0, 1$ since multiplicative identity is not guaranteed

## Subrings

**Subring**: subset $S$ of $R$ such that $S$ is a ring itself under operations of $R$

**Thereom 12.3**: Subring Test - $S$ is a subring if it is closed under subtraction and multiplication ($a, b \in S \implies a - b, ab \in S$)

- Proof: since $R$ is commutative and $S$ is closed under subtraction, by One-Step Subgroup Test, $S$ is an Abelian group under addition

  Furthermore, multiplication in $R$ is associative and distributes over addition. Thus this must also be true for $S$

  Finally, multiplication is closed under $S$, so it must be a binary operation

**Examples**:

- $\{0\}$ and $R$ are subrings of ring $R$
- $\{0, 2, 4\}$ subring of $\mathbb{Z}_6$
  - Note that 1 is the unity in $Z_6$ but 4 is the unity in $\{0, 2, 4\}$
- For positive integer $n$, we have $n\mathbb{Z}$ is a subring of $\mathbb{Z}$
- $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring under $\mathbb{C}$

- $\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{Z}\}$ is a subring of $M_2(\mathbb{Z})$

# Integral Domains

**Zero Divisor**: nonzero element $a$ of a commutative ring $R$ such that there is a nonzero $b \in R$ with $ab = 0$

**Integral Domain**: commutative ring with unity and no zero divisors

- Product is $ab = 0$ only when $a = 0$ or $b = 0$

**Examples**

- Ring of integers is an integral domain
- Ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is an integral domain
- Ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is an integral domain
- Ring $\mathbb{Z}[x]$ of polynomials with integer coefficients is an integral domain
- Ring $\mathbb{Z}_p$ of integers modulo prime $p$ is an integral domain
- Ring $\mathbb{Z}_n$ of integers modulo $n$, not prime, is NOT an integral domain
- Ring $M_2(\mathbb{Z})$ is NOT an integral domain
- $\mathbb{Z} \oplus \mathbb{Z}$ is NOT an integral domain

**Theorem 13.1**: let $a, b, c$ belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$

- Proof: from $ab = ac \implies a(b - c) = 0$. Since $a \neq 0$ and $R$ is an integral domain, we must have $b - c = 0 \implies b = c$

## Fields

**Field**: commutative ring with unity where every nonzero element is a unit

- Every field is an integral domain since for $a \neq 0, ab = 0 \implies b = a^{-1}0 = 0$
- $ab^{-1}$ can be treated as $a$ divided by $b$
- Field can be thought of as an algebraic system closed under $+, -, \times, \div$

**Theorem 13.2**: Finite integral domain is a field

- Proof: let $D$ be a finite integral domain with unity 1 and let $a \in D$ be nonzero. We show $a$ is a unit If $a = 1$, then $a = a^{-1} = 1$ done

  Otherwise $a \neq 1$, so we have $a, a^2, a^3, \ldots$ Since $D$ is finite, we must have integers $i, j$ with $i > j$ such that $a^i = a^j$

  Then we have $a^{i-j} = 1$. Since $a \neq 1 \implies a^{-1} = a^{i-j-1}$

**Corollary**: $Z_p$ is a Field

- Proof: $Z_p$ clearly has unity, so from Theorem 13.2, we just need to show $Z_p$ has no zero divisors

  Take $a, b \in Z_p$ and $ab = 0$. Then $ab = pk$, but by Euclid's Lemma, either $p \mid a$ or $p \mid b$, but under $Z_p$, these are 0

**Examples**:

- $\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\} = \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\}$ is a field
- $Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\}$ is a field

  Clearly it's a ring. Inverses have the form $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a+b\sqrt{2}}$

## Characteristic of a Ring

**Characteristic of Ring**: least postiive integer $n$ such that $\forall x \in R, nx = 0$. If no integer exists, $R$ has characteristic 0

**Examples**

- $\mathbb{Z}$ has characteristic 0
- $\mathbb{Z}_n$ has characteristic $n$
- $\mathbb{Z}_2[x]$ has characteristic 2, even though it is an infinite ring

**Theorem 13.3**: Let $R$ be a ring with unity 1. If 1 has infinite order under addition, $R$ has characteristic 0. Otherwise $R$ has characteristic $n$

- Proof: If 1 has infinite order, then no positive integer $n$ exists such that $n \cdot 1 = 0 \implies R$ has characteristic 0

  If 1 has additive order $n$, then $n \cdot 1 = 0 \implies n$ is the least postiive integer with this property

  For any $x \in R$, we have $n \cdot x = 1x + 1x + \cdots + 1x = (1 + 1 + \cdots + 1)x = (n \cdot 1)x = 0x = 0$. Thus $R$ has characteristic $n$

**Theorem 13.4**: characteristic of an integral domain is 0 or prime

- Proof: from Theorem 13.3, it suffices to show that if the additive order of 1 is finite, it must be prime

  Suppose 1 has order $n$ and that $n = st$, then for $1 \leq s, t \leq n$, we have $0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1)$

  Thus $s \cdot 1 = 0$ or $t \cdot 1 = 0$. Since $n$ is the least positive integer with property $n \cdot 1 = 0$, either $s = n$ or $t = n$. Thus $n$ is prime

**Nilpotent**: $a \in R$ is **nilpotent** if there exists an positive $n$ such that $a^n = 0$

**Idempotent**: $a \in R$ is **idempotent** if $a^2 = a$

# Ideals and Factor Rings

**Ideal**: A subring $A$ of ring $R$ such that $\forall r \in R, a \in A$, both $ra, ar \in A$

- So the subring $A$ absorbs elements from $R$: $rA \subseteq A$ and $Ar \subseteq A$

**Theorem 14.1**: A nonempty subset $A$ of ring $R$ is an ideal of $R$ if

1. $a, b \in A \implies a - b \in A$
2. $ra, ar \in A$ when $a \in A, r \in R$

**Examples**:

- $\{0\}, R$ are both ideals of $R$
- $nZ$ is an ideal of $Z$
- Let $R$ be a commutative ring with unity and $a \in R$. The set $\langle a \rangle = \{ra \mid r \in R\}$ is the **principal ideal generated by** $a$
  - Commutativity is necessary
- Let $A$ denote the subset of all polynomials with constant term 0. Then $A$ is ideal of $\mathbb{R}[x]$ and $A = \langle x \rangle = \{a_1 x + \cdots + a_n x^n\}$
- Let $R$ be a commutative ring with unity and $a_1, \ldots, a_n \in R$. Then $I = \langle a_1, \ldots a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\}$ is the **ideal generated by** $a_1, \ldots, a_n$
- Take $I \subseteq Z[x]$. $I$ contains polynomials with an even constant term. Then $I$ is ideal and $I = \langle x, 2 \rangle = \{(a_n x^{n-1} + \cdots + a_1)x + 2k\}$
- Let $R$ be a ring of all real-valued functions and $S \subseteq R$ with all differentiable functions. Then $S$ is a subring of $R$ but NOT ideal.

  We can take $s$ differentiable and $r$ not-differentiable. Then $sr$ could be NOT differentiable

## Factor Rings

Take ring $R$ and ideal $A$ of $R$. Since $R$ is a group under addition and $A \trianglelefteq R$, we can create the factor group $R/A = \{r + A \mid r \in R\}$. Question is if we can form a ring of this group of cosets

- Addition properties are already taken care of
- Multiplicative properties requires $A$ be ideal

**Theorem 14.2**: let $R$ be a ring and $A$ be a subring of $R$. The sets of cosets is a ring under $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if $A$ is an ideal of $R$

- Proof: We know that cosets form a group under addition so we need to show that multiplication is well defined if and only if $A$ is an ideal of $R$
  - Suppose $A$ is an ideal of $R$ and let $s + A = s' + A$ and $t + A = t' + A$. We show that $st + A = s't' + A$

    By definnition we have that $s = s' + a$ and $t = t' + b$ for $a, b \in A$

    Thus we have $st = (s' + a)(t' + b) = s't' + at' + s'b + ab$

    Adding $A$ to both sides we get

$st + A = s't' + A$ since $A$ absorbs $at', s'b, ab$

- On the other hand, suppose $A$ is a subring but NOT ideal. Then there exists $a \in A, r \in R$ such that $ar \notin A$ or $ra \notin A$

  Consider $a + A = 0 + A$ and $r + A$

  Clearly $(a + A)(r + A) = ar + A$

  But $(0 + A)(r + A) = A \neq ar + A$

  Thus multiplication is not well defined under multiplication when $A$ is NOT ideal

Final steps involve showing multiplication is associative and multiplication distributes over addition

**Examples**:

- $Z/4Z = \{0 + 4Z, 1 + 4Z, 2 + 4Z, 3 + 4Z\}$

  $(2 + 4Z) + (3 + 4Z) = 1 + 4Z$

  $(2 + 4Z) \cdot (3 + 4Z) = 2 + 4Z$

- Let $R = \{\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \mid a_i \in Z\}$ and let $I$ be a subset of $R$ with even entries

  Clearly $I$ is an ideal of $R$. Also by analysis, we see that $R/I$ has size 16

  $\begin{bmatrix} 7 & 8 \\ 4 & -4 \end{bmatrix} + I = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + I$

- Consider $R = Z[i]/\langle 2 - i\rangle$ that has elements of the form $a + bi + \langle 2 - i\rangle$

  Since $2 - i + \langle 2 - i\rangle = 0 + \langle 2 - i\rangle$, we have $2 - i \equiv 0 \implies 2 = i$

  So $3 + 4i + \langle 2 - i\rangle = 11 + \langle 2 - i\rangle$

  We can reduce this further since $2 = i \implies 4 = -1 \implies 5 = 0$

  So $3 + 4i + \langle 2 - i\rangle = 11 + \langle 2 - i\rangle = 1\langle 2 - i\rangle$

- Consider $\mathbb{R}/\langle x^2 + 1\rangle = \{g(x) + \langle x^2 + 1\rangle \mid g(x) \in \mathbb{R}[x]\} = \{ax + b + \langle x^2 + 1\rangle \mid a, b \in \mathbb{R}\}$

  Last part of the equality comes from writing $g(x) = q(x)(x^2 + 1) + r(x)$. In particular, either $r(x) = 0$ or it has degree less than 2 $\implies r(x) = ax + b$

  Furthermore we have that $x^2 + 1 = 0 \implies x^2 = -1$ so for multiplication we have

  $(x + 3 + \langle x^2 + 1\rangle) \cdot (2x + 5 + \langle x^2 + 1\rangle) = 2x^2 + 11x + 15 + \langle x^2 + 1\rangle = 11x + 13\langle x^2 + 1\rangle$

## Prime and Maximal Ideals

**Prime Ideal**: proper ideal $A$ of $R$ such that $a, b \in R$ and $ab \in A \implies a \in A$ or $b \in A$

**Maximal Ideal**: proper ideal $A$ of $R$ such that when $B$ is an ideal of $R$ and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$

- So only the only ideal that properly contains a maximal ideal is the entire ring itself

**Examples**:

- Let $n$ be an integer other than 1. Then in the ring of integers, $nZ$ is prime if and only if $n$ is prime
- Ideal $\langle x^2 + 1\rangle$ is maximal in $\mathbb{R}[x]$

  Assume $A$ is deal of $\mathbb{R}[x]$ and properly contains $\langle x^2 + 1\rangle$

  **TODO FINISH THIS**
- Ideal $\langle x^2 + 1\rangle$ is NOT prime in $Z_2[x]$ since it contains $(x + 1)^2 = x^2 + 1$ but doesn't contain $x + 1$

**Theorem 14.3**: Let $R$ be a commutative ring with unity and $A$ be an ideal of $R$. Then $R/A$ is an integral domain if and only if $A$ is prime

- Proof:

  $\implies$ Suppose $R/A$ is an integral domain and $ab \in A$. Then $(a + A) \cdot (b + A) = ab + A = A \implies ab$ is the zero element in ring $R/A$

  So either $a + A = A$ or $b + A = A$, which means that either $a \in A$ or $b \in A$. Thus $A$ is prime

$\Longleftarrow$ Observe that $R/A$ is a commutative ring with unity for any proper ideal $A$. We show when $A$ is prime, then $R/A$ has no zero divisors

Suppose that $A$ is prime and $(a + A)(b + A) = 0 + A = A$. Then $ab \in A$ and $a \in A$ or $b \in A$

Thus either $a + A$ or $b + A$ is the zero coset in $R/A$

**Theorem 14.4**: Let $R$ be a commutative ring with unity and $A$ be an ideal of $R$. Then $R/A$ is a field if and only if $A$ is maximal

**TODO DO PROOF**

**Examples**:

- Ideal $\langle x \rangle$ is prime ideal in $Z[x]$ but is not a maximal ideal in $Z[x]$

  $\langle x \rangle = \{f(x) \in Z[x] \mid f(0) = 0\}$

  Thus $g(x)h(x) \in \langle x \rangle \implies g(0)h(0) = 0 \implies g(0) = 0$ or $h(0) = 0$

  Not maximal because $\langle x \rangle \subset \langle x, 2 \rangle \subset Z[x]$