Math 1530: Abstract Algebra

Milan Capoor

Fall 2023

Groups

Lecture 1: Sept 7

Richard Schwartz

- richard.evan.schwartz@gmail.com

The Cube

Let G be the set of symmetries of the cube. Given $a,\ b \in G$, $a \star b$ is the concatenation of a and b

Notice:

- $(a \star b) \star c = a \star (b \star c)$ (associative)
- $\exists e$ such that $e \star a = a \star e = a \ \forall a \in G$ (identity)
- $\forall a \in G \ \exists b$ such that $a \star b = e$ (inverse)

A group is anything that satisfies these axioms

Examples of groups:

- Permutations of the Rubik's Cube
- the integers
- $\mathbb{Z}//n := \{0, \ldots, n-1\}$ ("Z mod n" where $Z//12$ would work like a clock)

Structures heuristically:

- A group is a set with addition/concatenation
- A ring is a group plus multiplication

- A field is a ring plus division and commutativity

Lecture 2: Sept 12

Groups

Group: a group is a set G with an operation $\star : G \times G \to G$ such that

1. $\star$ is always defined
2. $a \star (b \star c) = (a \star b) \star c \quad \forall a, b, c \in G$ (Associativity)
3. $\exists e \in G,$ such that $e \star a = a \star e = a \quad \forall a \in G$ (Identity)
4. $\forall a \in G,\ \exists b \in G,$ such that $a \star b = b \star a = e$ (Inverses)

Lemma 1: In a group, e is unique.

Proof:

1. Suppose e and e' are both identity elements of the group G.
2. Consider $e \star e'$
3. Since e is an identity, $e \star e' = e'$
4. But since e' is an identity, $e \star e' = e$
5. Therefore, $e' = e \quad \blacksquare$

Lemma 2: Suppose $a \star c_1 = a \star c_2$. Then, $c_1 = c_2$.

Proof:

1. Let b be an inverse of a
2. Since $a \star c_1 = a \star c_2$,
$$b \star (a \star c_1) = b \star (a \star c_2)$$
3. Then by associativity,
$$(b \star a) \star c_1 = (b \star a) \star c_2$$
4. By the definition of inverses, $(b \star a) = e$ so
$$e \star c_1 = e \star c_2$$

5. And by identity,
$$c_1 = c_2 \quad \blacksquare$$

Lemma 3: Inverses are unique ($\forall a \in G \quad \exists! b \in G$ such that $a \star b = b \star a = e$)

Proof:

1. Suppose b_1 and b_2 are both inverses of a
2. Then,
$$a \star b_1 = e = a \star b_2$$
3. By lemma 2, $b_1 = b_2 \quad \blacksquare$

Examples of Groups

Permutation groups: The set of all bijective maps from $S \to S$ (the maps that hit every element in the codomain exactly once)

Surjective: onto; each element of the codomain is mapped to by at least one element of the domain.

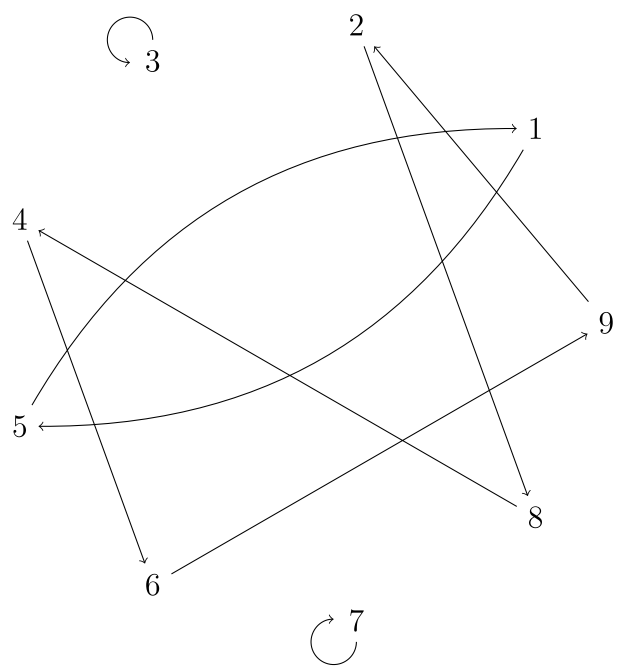
Injective: one-to-one; each element of the codomain is mapped to by at most one element of the domain

Permutation groups can be represented by arrow diagrams, tables, pairs, and cycles. For example,

S	$g(S)$
1	5
2	8
3	3
4	6
5	1
6	9
7	7
8	4
9	2

is the same as
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 3 & 6 & 1 & 9 & 7 & 4 & 2 \end{pmatrix}$$

which is also equivalent to



which can be notated

$$(3)(7)(15)(28469)$$

Homomorphisms

Homomorphism: a map between groups G_1 and G_2, $\phi : G_1 \to G_2$ such that $\phi(a \star_1 b) = \phi(a) \star_2 \phi(b)$

Example: G_1 is rotations of a pentagon and $G_2 = \mathbb{Z}/5$

Isomorphism: a bijective homomorphism

Lecture 3: Sept 14

Recall: a homomorphism is a map $\phi : G_1 \to G_2$:

$$\phi(a \star_1 b) = \phi(a) \star_2 \phi(b)$$

Lemma: Let ϕ be a homomorphism from $G_1 \to G_2$. Then $\phi(g^{-1}) = (\phi(g))^{-1} \quad \forall g \in G_1$

Proof:

$$\begin{aligned}
\phi(e) &= e \\
g \cdot g^{-1} &= e \\
e = \phi(g \cdot g^{-1}) &= \phi(g) \cdot \phi(g^{-1}) && \text{by homomorphism} \\
e &= \phi(g) \cdot (\phi(g))^{-1} && \text{by definition of inverse} \\
\phi(g^{-1}) &= (\phi(g))^{-1} && \text{by cancellation} \quad \blacksquare
\end{aligned}$$

Subgroups

Kernel: Let $\phi : G_1 \to G_2$ be a homomorphism. Then

$$\ker(\phi) := \phi^{-1}(e) = \{a \in G_1 | \phi(a) = e\}$$

Lemma: $\ker(\phi)$ is a subgroup of G_1

Proof:

1. Suppose $a, b \in \ker(\phi)$

$$\phi(ab) = \phi(a)\phi(b) = ee = e \quad \checkmark$$

2. Suppose $a^{-1} \in \ker(\phi)$

$$\phi(a^{-1}) = [\phi(a)]^{-1} = e^{-1} = e \quad \checkmark$$

Therefore $\ker(\phi)$ is closed under multiplication and inverses, so it is a subgroup. $\blacksquare$

Theorem: ϕ is one-to-one (injective) if and only if $\ker(\phi) = \{e\}$

Proof:

$\phi(e) = e$ so $\phi(g) \neq e$ if $g \neq e$. Therefore, $\ker(\phi)$ must be $\{e\}$

Now for the other direction, suppose $\phi(x) = z$ and $\phi(y) = z$. We then know $\phi(y^{-1}) = z^{-1}$, so

$$\phi(y^{-1})\phi(x) = z^{-1}\phi(x) = z^{-1}z = e$$

Because ϕ is a homomorphism,

$$\phi(y^{-1})\phi(x) = \phi(y^{-1}x)$$

so

$$y^{-1}x \in \ker(\phi) \implies y^{-1}x = e \implies x = y \quad \blacksquare$$

More generally

Let $\phi : G_1 \to G_2$ be a homomorphism and H_2 a subgroup of G_2,

$$\phi^{-1}(H_2) = \{a \in G_1 | \phi(a) \in H_2\}$$

Lemma: $\phi^{-1}(H_2)$ is a subgroup of G_1

Proof:

1. Identity: $\phi(e) = e \quad e \in \phi^{-1}(H_2)$
2. Multiplication closure: $a, b \in \phi^{-1}(H_2)$,

   $$\phi(ab) = \phi(a)\phi(b) \in H_2 \qquad H_2 \text{ is closed under products}$$

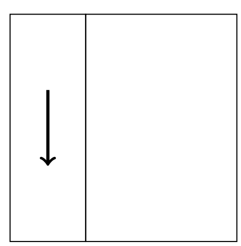
   so $ab \in \phi^{-1}(H_2)$
3. Inverse closure: $a \in \phi^{-1}(H_2)$

   $$\phi(a^{-1}) = [\phi(a)]^{-1} \in H_2 \qquad H_2 \text{ is closed under inverses}$$

   so $a^{-1} \in \phi^{-1}(H_2)$

Interlude: Cube notation

Let

$a =$ 

This means that we turn the left face down.

Notice that after four turns, we have returned to the beginning, so

$$aaaa = a^4 = e$$

which creates a (cyclic) subgroup of the cube,

$$H = \{e, a, a^2, a^3\}$$

Notation: Given G and $a \in G$,

$$\langle a \rangle = \{a^k,\ k \in \mathbb{Z}\}$$

,

Why are the symmetries of the cube not a cyclic group?

There is no generator of order 24.

OR cyclic groups are abelian.

$$a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$$

Lecture 4: Sept 19

Review

Recall: A homomorphism is a map $\phi : G_1 \to G_2$ such that

$$\begin{aligned} \phi(ab) &= \phi(a)\phi(b) \\ \phi(e_1) &= e_2 \\ \phi(g^{-1}) &= (\phi(g))^{-1} \end{aligned}$$

To confirm H is a subgroup: check that it is closed under multiplication and inverses. You do not need to show associativity because that is always true.

Generators: Let $G = \{a, a^2, a^3, \dots\}$ If $a^m = a^n \quad m < n$ then

$$\begin{aligned} a^{n-m} &= e \\ a^k = e \qquad (k &= n-m) \\ (a^{k-1})a &= e \\ a^{k-1} &= a^{-1} \end{aligned}$$

Are Abelian Groups always cyclic? *Answer:* No. Counterexample:

$$\mathbb{Z}/2 \times \mathbb{Z}/2 = \{(a,b)|\ a, b \in \mathbb{Z}/2\} = \{(0,0),(0,1),(1,0),(1,1)\}$$

has no generator.

(Left) Cosets

Definition: Given a group G and a subgroup $H \subset G$, a *left coset* is a set of the form

$$aH = \{ah \mid h \in H\}$$

where $a \in G$

If $a \in H$, then $aH = H$. (Notice that for all $s \in H$, $a(a^{-1}s) = s$ and $a^{-1}s \in H$)

This all leads to the observation that *every set of cosets contains the subgroup.*

Lemma: H and aH are the same size (there is a bijection from H to aH)

Proof: Define $\psi(h) = ah$. By definition, $aH = \psi(H)$ so ψ is onto. Now suppose $\psi(h_1) = \psi(h_2)$. Then $ah_1 = ah_2$ which by cancellation shows $h_1 = h_2$. Thus, ψ is one-to-one. Therefore, $\psi : H \to aH$ is a bijection. ∎

Lemma: If $aH \cap bH \neq \emptyset$, then $aH = bH$.

Proof: Pick an element in common: $ah_1 = bh_2$. Then

$$a = bh_2h_1^{-1}$$

so for any $h \in H$,

$$ah = b(h_2h_1^{-1}h) \in bH$$

Since this is true for all $h \in H$, we know that $aH \subset bH$.

Interchanging a and b shows that $aH = bH$. ∎

Lagrange's Theorem

Theorem: If G is a finite group and $H \subset G$ is a subgroup, then $o(H) | \, o(G)$ (The order of H divides the order of H.)

Proof: Look at all the cosets and denote the number of cosets n. We know

1. For any $g \in G$, $g = ge \in gH$ (every element is in a coset)
2. All cosets have $o(H)$ elements (from the bijection)
3. The cosets are mutually exclusive

So $o(G) = n \cdot o(H)$ ∎

Corollary: If $g \in G$ and G is a finite group, then $o(g)|o(G)$

Proof: Let $H = \langle g \rangle$. Then $o(H) = o(g)$. Since $o(H)|\ o(G)$ (by Lagrange's), $o(g)|\ o(G)$. ■

Lecture 5: Sept 21

Recall

Lagrange's Theorem: $H \subset G \implies o(H)|\ o(G)$

Corollary of Lagrange's Theorem: if $g \in G$, $o(g)|\ o(G)$

Equivalence Relations

Relation: a relation on a set S is a subset $R \in S \times S$

$$x\ R\ y \implies (x, y) \in R$$

Equivalence Relation: a relation $x \sim y$ such that $(x, y) \in R$ and

1. $x \sim x \quad \forall x \in S$
2. $x \sim y \implies y \sim x \quad \forall x, y \in S$
3. $x \sim y,\ y \sim z \implies x \sim z \quad \forall x, y, z \in S$

Example: $H \subset G$ with $a \sim b$ if $a^{-1}b \in H$

$$a \sim a \implies a^{-1}a \in H \implies e \in H\checkmark \tag{1}$$
$$a \sim b \implies a^{-1}b \in H \implies (a^{-1}b)^{-1} = (b^{-1}a)^{-1} \implies b \sim a\checkmark \tag{2}$$
$$a \sim b,\ b \sim c \implies a^{-1}b, b^{-1}c \in H \implies a^{-1}x \in H \implies a \sim c\checkmark \tag{3}$$

Remark: if two equivalence classes overlap, they are the same *Proof:* an equivalence class is a coset

Example:

$$a^{-1}b \in H$$
$$a^{-1}b = h \in H$$
$$b = ab \in aH$$

The group $(\mathbb{Z}/n)^*$

Relatively Prime: $a, b \in \mathbb{Z}$ are *relatively prime* if $\gcd(a, b) = 1$

Lemma: if a, b are relatively prime then $\exists s, t$ such that

$$as + bt = 1$$

Proof:

$\Longleftarrow$ suppose $as + bt = 1$ and d divides a, b. Clearly, $d|as$ and $d|bt$ for $s, t \in \mathbb{Z}$. By distribution,

$$d|as + bt = 1 \implies d|1 \implies d = 1$$

$\Longrightarrow$ Let a, b be the smallest pair with $a < b$. Consider $a, b - a$. If a and $b - a$ are relatively prime, then

$$s'a + t'(b - a) = 1 = (\underbrace{s' - t'}_{s})a + \underbrace{t'}_{t} b = 1$$

To show that a and $b-a$ are relatively prime, we suppose $d|a$ and $d|b-a$ so $d|a+(b-a)$ so $d|b$. Using the first part of the proof, we know have $as + bt = 1$ for the smallest pair we did not know we could write that way. Thus it is true for all numbers.

Definition: $(\mathbb{Z}/n)^*$ is the subset of $\{1, \dots, N\}$ which is relatively prime to N together with group law multiplication and reduction.

$$(\mathbb{Z}/15)^* = \{1, 2, 4, 7, 8, 11, 13, 13, 14\}$$

Example: $7 \cdot 8 = 56 - (15 * 3) = 11 \in (\mathbb{Z}/15)^*$

We now consider $a, b \in (\mathbb{Z}/15)^*$

$$\begin{cases} 1 = s_1 a + t_1 N \\ 1 = s_1 b + t_2 N \\ 1 = s_1 s_a v + \dots N \end{cases} \implies ab \in (\mathbb{Z}/15)^*$$

(so identity)

Inverses in $(\mathbb{Z}/N)^*$:

$$\begin{aligned} a &\in (\mathbb{Z}/15)^* \\ as + tN &= 1 \\ s &= a^{-1} \\ aa^{-1} + tN &= 1 \end{aligned}$$

(so inverses mod multiples are in the group)

Order of $(\mathbb{Z}/15)^*$:

$$\phi(n) := o(\mathbb{Z}/15)^*$$

We have $\phi(15) = 8$, $\phi(17) = 16$, etc.

In general, if p is prime then $\phi(p) = p - 1$ and if p, q are prime then $\phi(pq) = (p-1)(q-1)$

$$\boxed{\frac{\phi(N)}{N} = \prod_{p|n} 1 - \frac{1}{p}}$$

Example: $N = 12, \quad (\mathbb{Z}/12)^* = \{1, 5, 7, 11\}$

$$\frac{\phi(12)}{12} = (1 - \frac{1}{2})(1 - \frac{1}{3}) = \frac{1}{3} \implies \phi(12) = 4$$

RSA Cryptography

Corollary of Lagrange's Theorem: If a is relatively prime to N then

$$a^{\phi(N)} \equiv 1 \mod n$$

The Algorithm:

1. Pick two very large primes p, q (choose very big numbers and check if they are prime)
2. publish the value of $N = pq$
3. Keep secret the number $\phi(N) = (p-1)(q-1)$
4. Choose a public E relatively prime to $\phi(N)$ $(DE + k\phi(N) = 1)$ where D is your private "decoder"

Rings

Lecture 6: Sept 26

Ring: a set R with two operations (usually $+$, $\cdot$) such that:

1. $(R, +)$ is an abelian group
2. $(R, \cdot)$ is a "group" which may or may not have inverses (the operation is always defined, it is associative, and there is an identity)
3. $$\forall a, b, c \in R: \quad \begin{cases} a \cdot (b + c) = a \cdot b + a \cdot c \\ (b + c) \cdot a = b \cdot a + c \cdot a \end{cases}$$

We usually call 1 the multiplicative identity (the identity for the operation $\cdot$) and 0 the additive identity (the identity for $+$)

Lemma: $0 \cdot a = a \cdot 0 = 0 \quad \forall a \in R$

Proof:

$$0 + 0 = 0 \implies (0 + 0) \cdot a = 0a + 0a = 0 \cdot a$$

By the additive inverse,

$$-0a + 0a + 0a = -0a + -0a \implies 0a = 0 \quad \blacksquare$$

Lemma: $(-a) \cdot b = -(a \cdot b)$

Proof:

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

Examples of Rings

- The integers $(\mathbb{Z}, +, \cdot)$
- $\mathbb{Z}/n$
- $Z[x]$ (the set of integer polynomials $a_0 + a_x + \cdots + a_n x^n$)
- $\mathbb{Z}/6[x]$ (polynomials with coefficients in $\mathbb{Z}/6$)
- $(R[x])[y]$ (the ring of polynomials in y whose coefficients are elements in $R[x]$)
- $R[x, y] = \{\sum a_{ij} x^i y^k | \; a_{ij} \in R\}$ (this is isomorphic to the example above)
- $M_n(R)$ is the $n \times n$ matrix ring with coefficients in R
- $\mathbb{Z}[i] = \{a + bi | \; a, b \in \mathbb{Z}, i^2 = -1\}$ (the Gaussian integers)
- $\mathbb{Z}[\omega] = \{a + b\omega \mid \omega = e^{2\pi i/3}\}$ (Eisenstein integers)

Ring Homomorphisms

Definition: $\phi : R_1 \to R_2$ is a ring homomorphism iff

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$
3. $\phi(1) = 1$

Examples of homomorphisms:

- $\phi : \mathbb{Z} \to \mathbb{Z}/n \longrightarrow \phi(k) = k \mod n$
- $\phi : \mathbb{Z}/mn \to \mathbb{Z}/n$

$\mathbb{Z}/6$	$\mathbb{Z}/3$
0	0
1	1
2	2
3	0
4	1
5	2

Lecture 7: Sept 28

Review

Ring: a set with two operations $(R, +, \cdot)$ where $(R, +)$ is an abelian group, $(R, \cdot)$ follows all the group axioms except (potentially) inverses, and

$$a(b + c) = ab + ac$$

Ring Homomorphism: $\phi : R_1 \to R_2$ where

$$\begin{aligned}\phi(a + b) &= \phi(a) + \phi(b)\\ \phi(ab) &= \phi(a)\phi(b)\\ \phi(1) &= 1\end{aligned}$$

More examples:

- $\phi : \mathbb{Z} \to R_2$ is a unique homomorphism ($\phi(1) = 1$, $\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 2, \dots$)
- Similarly, (if it exists) $\mathbb{Z}/n \to \mathbb{R}$ will be unique
- $\phi : \mathbb{C} \to \mathbb{C}$. One homomorphism is $\phi(x + iy) = x + iy$. But $\phi(x + iy) = x - iy$ is also a homomorphism

  Lemma: $\phi(ab) = \phi(a)\phi(b)$

  Proof:

  $$\begin{aligned}(a + bi)(c + di) &= ac - bd + i(ad + bc)\\ (a - bi)(c - di) &= ac - bd - i(ad + bc)\end{aligned}$$

- $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \ \mid Z\},\ \phi(a + b\sqrt{2}) = a - b\sqrt{2}$

Unit group

Unit: an element of a commutative ring with an inverse. i.e.,

$$a, b \in R : ab = 1$$

Lemma: $(R^\star, \cdot)$ is a group (where $R^\star$ is the set of units of R)

Proof:

1. The units are closed under composition

$$1 = aa' = bb' \implies 1 = aa'bb' = (ab)(a'b')$$

2. $R^\star \subset R$ is a ring so associativity holds
3. We have an identity because $1 \in R^\star$
4. We have inverses because $ab = 1 \implies ba = 1$

Example: $(\mathbb{Z}/N)^\star$ = set of elements relatively prime to N

Because $(\mathbb{Z}/N)^\star$ is a group, all its elements have inverses so

$$(\mathbb{Z}/N)^\star \subset (\mathbb{Z}/N)^\sharp$$

(where $(\mathbb{Z}/N)^\sharp$ is the unit group)

Now let

$$ab = 1 \quad \in \mathbb{Z}/N \tag{4}$$
$$b = kN + 1 \quad \in \mathbb{Z} \tag{5}$$
$$ab - KN = 1 \implies ab \text{ is relatively prime to } N \tag{6}$$

So a is relatively prime to N so

$$(\mathbb{Z}/N)^\sharp \subset (\mathbb{Z}/N)^\star \implies (\mathbb{Z}/N)^\sharp = (\mathbb{Z}/N)^\star$$

Products of Rings

Definition:

$$R_1 \times R_2 = \{(a_1, a_2) \mid a_1 \in R_1,\ a_2 \in R_2\}$$

with

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \tag{7}$$
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2) \tag{8}$$

Lemma: $(R_1 \times R_2^\star) = R_1^\star \times R_2^\star$

If we have units in R_1, R_2, then

$$(a_1, a_2) \cdot (b_1, b_2) = (1, 1)$$

Lecture 8: Oct 3

Special Cases of Rings

Field: $(R - \{0\}, \cdot) = R^*$ is an abelian group (every non-zero element has an inverse)

Integral Domain: A commutative ring where $ab = 0 \implies a = 0$ or $b = 0$

Ideals

Definition: An *ideal* $I \subset R$ is a subgroup under addition of R and has the "absorption property" such that

$$\forall a \in I, r \in R : ar \in I$$

Not an Ideal:

- $I = \mathbb{R}$, $R = \mathbb{R}[x]$
- $I = \{(n, n) \big| n \in \mathbb{Z}\},\ R = \mathbb{Z} \times \mathbb{Z}$

Ideals:

- $I = 2\mathbb{Z}, \quad R = \mathbb{Z}$
- $I = \{(n, 0) \big| n \in \mathbb{Z}\}, \quad R = \mathbb{Z} \times \mathbb{Z}$

Principal Ideals: Given $a \in R$,

$$aR = \{ar \mid r \in R\}$$

Proof this is an ideal:

- Distribution: $ab_1 + ab_2 = a(b_1 + b_2)$
- Absorption: $s \in R,\ s(ar) = a(sr)$
- Inverse: $-ab = a(-b)$
- Additive identity: $a0 = 0$

An ideal that is not a principal ideal:

- (General case) All finite sums $\sum_i a_i r_i$ with $a_1, \ldots,\ a_n, r_i \in R$

  Observe
$$r\left(\sum_i a_i r_i\right) = \sum_i a_i (r r_i)$$

Quotients

Quotient ring: a ring $\mathbb{R}/I$ from commutative ring R and ideal $I \in R$

The elements of R/I are the cosets of I,
$$a + I, \quad a \in R$$

We have new group laws:
$$\begin{aligned}(a + I) + (b + I) &:= (a + b) + I \\ (a + I)(b + I) &:= (ab) + I\end{aligned}$$

Problem: what if a and b are redundant sets? When $R = \mathbb{Z},\ I = 2\mathbb{Z}$ we have $1 + 2\mathbb{Z} = 13 + \mathbb{Z}$ (the odd integers) but $1 \neq 13$

Lemma: If $a' + I = a + I$ and $b' + I = b + I$ then
$$(a + b) + I = (a' + b') + I$$

Proof:
$$\begin{aligned}a' &= a + i \qquad i \in I \\ b' &= b + j \qquad j \in I \\ a' + b' &\in (a' + b' + I) \\ a' + b' = a + b + (i + j) &\in (a + b) + I \\ (a + b + I) \cap (a' + b') + I &\neq \emptyset \\ \therefore (a + b) + I &= (a' + b') + I\end{aligned}$$

Lemma: If $a' + I = a + I$ and $b' + I = b + I$ then

$$a'b' + I = ab + I$$

Proof:

$$\begin{aligned}
a' &= a + i \\
b' &= b + i \\
a'b' &= (a + i)(b + j) \\
&= ab + ib + aj + ij
\end{aligned}$$

But by absorption, $ib + aj + ij \in ab + I$. so the rest follows from the same proof as above.

Showing Associativity:

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

Identity: $(a + I) + (0 + I) = a + I$