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
- $\mathbb{Z}//n := \{0,\ ..., n-1\}$ ("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.

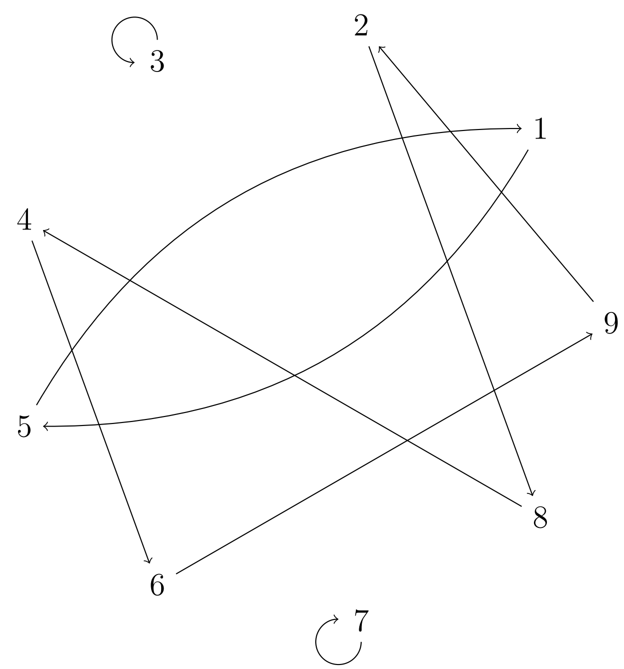
Injective: one-to-one; each element of the codomain is mapped to by at most one element of the domain

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: $a, b \in \phi^{-1}(H_2)$,

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

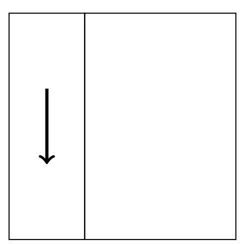
   so $ab \in \phi^{-1}(H_2)$
3. Inverse closure: $a \in \phi^{-1}(H_2)$

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

   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 $o(H) \mid o(G)$ (by Lagrange's), $o(g) \mid o(G)$. ■

Lecture 5: Sept 21

Recall

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

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

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:

$$\begin{aligned} a^{-1}b &\in H \\ a^{-1}b = h &\in H \\ b = ab &\in aH \end{aligned}$$

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,

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

$\implies$ 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 $\{1, \ldots, N\}$ 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 $a, b \in (\mathbb{Z}/15)^*$

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

(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 $+, \quad \cdot$) 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 $R[x]$)
- $R[x, y] = \{\sum a_{ij} x^i y^k \mid a_{ij} \in R\}$ (this is isomorphic to the example above)
- $M_n(R)$ is the $n \times n$ matrix ring with coefficients in R
- $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\}$ (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
  $$r\left(\sum_i a_i r_i\right) = \sum_i a_i(rr_i)$$

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

Inverse: $(a + I) + (-a + I) = (a - a) + I = 0 + I$

Lecture 9: Oct 5

Review

Ideal:

In a commutative ring, $I \subset R$ is an *ideal* if I is a subgroup under addition and I has the absorber property

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

Quotient:

We can then construct R/I which is the set of cosets of I (as an abelian group)

$$R/I = \{a + I, \quad a \in R\}$$

However, this construction can obscure the fact that a single coset can be constructed in many ways (for example with $I = 2\mathbb{Z}$, both $0 + I$ and $-30 + I$ are the evens).

Thus we confirm that the operations

$$\begin{aligned}(a + I) + (b + I) &:= (a + b) + I \\ (a + I) \cdot (b + I) &:= ab + I\end{aligned}$$

on R/I are well-defined (because two cosets that overlap are the same)

Examples:

- $R/I = \mathbb{Z}/5\mathbb{Z}$ has five distinct cosets:

  $$0 + 5\mathbb{Z},\ 1 + 5\mathbb{Z},\ 2 + 5\mathbb{Z},\ 3 + 5\mathbb{Z},\ 4 + 5\mathbb{Z}$$

  so it is isomorphic to $\mathbb{Z}/5 = \{0, 1, 2, 3, 4\}$

- $$R = \mathbb{R}[x] = \left\{ \sum_{i=0}^{n} a_i x^i : \quad a_i \in \mathbb{R}, n \in \{0, 1, 2, \dots\} \right\}$$

  with

  $$I = R(x^2 + 1) = \{p(x)(x^2 + 1),\ p(x) \in R\}$$

  gives the quotient ring R/I with elements like

  $$\begin{cases} n + I \quad \forall n \in \mathbb{N} \\ -x^2 + I = -x^2 + (x^2 + 1) + I = 1 + I \\ (x^3 - 5) + I = (x^2 + I)(x + I) + (-5 + I) = (-1 + I)(x + I) + (-5 + I) \\ \vdots \end{cases}$$

  More operations lead to the very strong conclusion: *every ideal can be written in the form*

  $$\boxed{(a + I) + (bx + I) \quad a, b \in \mathbb{R}}$$

  If we continue with this example, we can see

  $$(x + I)(x + I) = x^2 + I = -1 + I$$

  so in a sense $(x + I) = \sqrt{-1}$ and in fact this does define a ring isomorphism to the complex numbers!

- $R = \mathbb{Q}[x]$ and $I = R(x^2 - 2)$ allows us to define "$\sqrt{2}$"via

  $$(x + I)(x + I) = x^2 + I = x^2 - (x^2 - 2) + I = 2 + I$$

  This particular ring also happens to be a field.

Principal Ideal: the set of all multiples of an element in the ring

Homomorphisms and Ideals

Ring homomorphism: a map $\phi : R_1 \to R_2$ which respects both rings' operations:

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

Kernel:

$$\ker(\phi) = \{a \in R_1 \mid \phi(a) = 0\}$$

Lemma: $\ker(\phi)$ is an ideal

Proof: $\ker(\phi)$ is an abelian group since ϕ is also group homomorphism. Let $a \in I, r \in R$. Observe

$$\begin{aligned}\phi(ar) &= \phi(a)\phi(r) \quad \text{ring homomorphism}\\ &= 0 \cdot \phi(r) \quad a \in \ker\phi\\ &= 0\end{aligned}$$

So $ar \in I$. Thus $\ker\phi$ is an abelian group with absorption so it is a group.

Example:

Given R and I ideal, we construct

$$\pi : R \to R/I \implies \phi(a) = a + I$$

Therefore, $\ker\pi = I$

This can also be represented:

$$
\begin{tikzcd}
R_1 \arrow[r, "\phi"] \arrow[d, "\pi"'] & R_2 \\
R_1/I \arrow[ur, dashed, "\alpha"'] &
\end{tikzcd}
$$

with $I = \ker\phi$.

Does α exist? Observe:

$$
\begin{aligned}
\alpha(a+I) &= \phi(a) \\
\alpha(a'+I) &= \phi(a') \\
a' &= a+i \quad i \in I = \ker\phi \\
\phi(a') &= \phi(a+i) = \phi(a) + \phi(i) = \phi(a) + 0\phi(a)
\end{aligned}
$$

So the map α exists.

In fact,

$$\alpha(a+I) = 0 = \phi(a) \implies a \in \ker\phi = I$$

Thus

$$\ker\phi = \{I\} = 0$$

so ϕ iś injective.

Theorem: If $\phi : R_1 \to R_2$ is onto (surjective) $\alpha : R_1/I \to R_2$ is an R_2

Example: $R_1 = \mathbb{R}[x]$, $R_2 = \mathbb{C}$, and $\phi : R_1 \to R_2$.

$$\phi\left(\sum_{k=0}^{n} a_k x^k\right) = \sum_{k=0}^{n} a_k i^k = x + iy$$

So

$$\ker\phi = \{0,\ x^2+1,\ p(x)(x^2+1)\} = R_1(x^2+1)$$

(0 obviously, $x^2 + 1 = i^2 + 1 = 0$, and any multiple of 0)

Thus,

$$\mathbb{R}[x]/(\mathbb{R}[x](x^2+1)) \approxeq \mathbb{C}$$

Corollary: In general, $\alpha : R_1/I \to \mathrm{Im}(\phi)$ (where $\mathrm{Im}(\phi) = \phi(R_1)$) is an isomorphism.

Lecture 10: Oct 10

2 special kinds of Rings	2 special kinds of Ideals
Integral domains	Prime ideals
Fields	Maximal Ideals

Unsurprisingly, they are related! We will take them one-by-one and then connect them.

Integral Domain: R is an integral domain if

$$\forall a, b \in R : \quad ab = 0 \implies a = 0 \text{ or } b = 0$$

Not every ring is an integral domain. Consider $\mathbb{Z}/6$: $2 \cdot 3 = 0$

Prime Ideal: $I \subset R$ is a prime ideal if

$$\forall a, b \in R : \quad ab \in I \implies a \in I \text{ or } b \in I$$

Examples:

- $R = \mathbb{Z}, I = 2\mathbb{Z}$ is a prime ideal (product of an even and odd or even and even is even)
- $R = \mathbb{Z}, I = 10\mathbb{Z}$ is NOT a prime ideal ($2 \notin I, 5 \notin I, 10 \in I$)
- $R = \mathbb{Z}[i], I = 5R$ is NOT an ideal (despite 5 being prime) because $1 \pm 2i \notin I, (1+2i)(1-2i) = 5 \in I$

Generally, $n\mathbb{Z}$ is a prime ideal precisely when n is prime.

Theorem: R/I is an integral domain if and only if I is a prime ideal.

Proof:

We want to show that both directions are true. First consider the lemma that I is prime if R/I is an integral domain.

Suppose $ab \in I$ (so $ab + I = 0 + I$). We seek to show that $a = 0$ or $b = 0$. Consider the cosets $a + I$ and $b + I$:

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

So

$$(a + I)(b + I) = 0 + I$$

Since R/I is an ID, $a + I = 0 + I$ or $b + I = 0 + I$ in R/I. So either $a \in I$ or $b \in I$. Hence, I is prime.

To see the other direction, first suppose I is prime. Then $a \in I$ or $b \in I$. So

$$(a + I)(b + I) = 0 \implies ab + I = 0 + I$$

Thus, $ab \in I$. Since I is prime, $a \in I$ or $b \in I$. This is equivalent to

$$(a + I = 0 + I) \vee (b + I = 0 + I)$$

So $a = 0$ or $b = 0$ and R/I is an integral domain. ■

Field: R is a field if $R^* = R - \{0\}$ (i.e. all non-zero elements have inverses)

Lemma: R is a field if the only ideals in R are $R, \{0\}$

Proof: Suppose R is a field and $I \neq \{0\}$ is an ideal. We want to show that $I = R$. Consider, $a \in I,\ a \neq 0$. Because R is a field, $b = a^{-1}$ exists. Further,

$$1 = ba \in I \quad \text{(by absorption)}$$

for any $r \in R$,

$$r = r1 \in I$$

Therefore, $I = R$.

Going the other direction, suppose R is a ring whose only ideals in R are R and $\{0\}$. We pick any $a \in R,\ a \neq 0$ and consider $I = aR$. Since

$$a1 = a \in I \quad I \neq \{0\}$$

But if $I \neq \{0\}$, then $I = R$ so $1 \in I$. Then for any $r \in R$, $r1 = r \in I$ so $r = a^{-1}$ exists for any a. Thus, R is a field.

Maximal Ideal: $I \subset R$ is a maximal ideal if there are no ideals J with $I \subset J \subset R$ (with these being proper subsets)

Examples:

- $6\mathbb{Z} \subset \mathbb{Z}$ is not a maximal ideal because $6\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$

Theorem: R/I is a field if and only if I is maximal.

Proof: There is a bijection between the set of ideals of R that contain I (A) and the set of ideals of R/I (B). (See Lecture 11). Then

$$\text{R/I field} \iff \#B = 2 \iff \#A = 2 \iff \text{I maximal}$$

Alternative Proof Structure:

Suppose I is maximal. We pick an ideal $\overline{J}$ of R/I. We want to show that $\overline{J} = \{[0]\}$ or $\overline{J} = R/I$. Consider $\pi : R \to R/I$ whose kernel is just I. Let $J = \pi^{-1}(\overline{J})$. J is an ideal because it has the absorber property. Further, $I \subset J$ because $I = \ker(\pi)$. Therefore, $I \subset J \subset R$. Since I is maximal, $J = I$ or $J = R$. If $J = I$, then $\overline{J} = \{[0]\}$. Similarly, if $J = R$, then $\overline{J} = \pi(R)$. So the only ideals in R/I are $\{0\}$ and R.

To see the other direction, assume the only ideals in R/I are $\{0\}$ and R. Try to find a subset $I \subset J \subset R$ with $J \neq I$ and $J \neq R$ but as the ...

Corollary: $\mathbb{Z}/p\mathbb{Z}$ is a field for p prime.

Proof: Show $p\mathbb{Z}$ is a maximal ideal.

$$p\mathbb{Z} \subsetneq J \subset \mathbb{Z}$$

Since $J \neq p\mathbb{Z}$ there must be an element $n \in J$ relatively prime to p. Then,

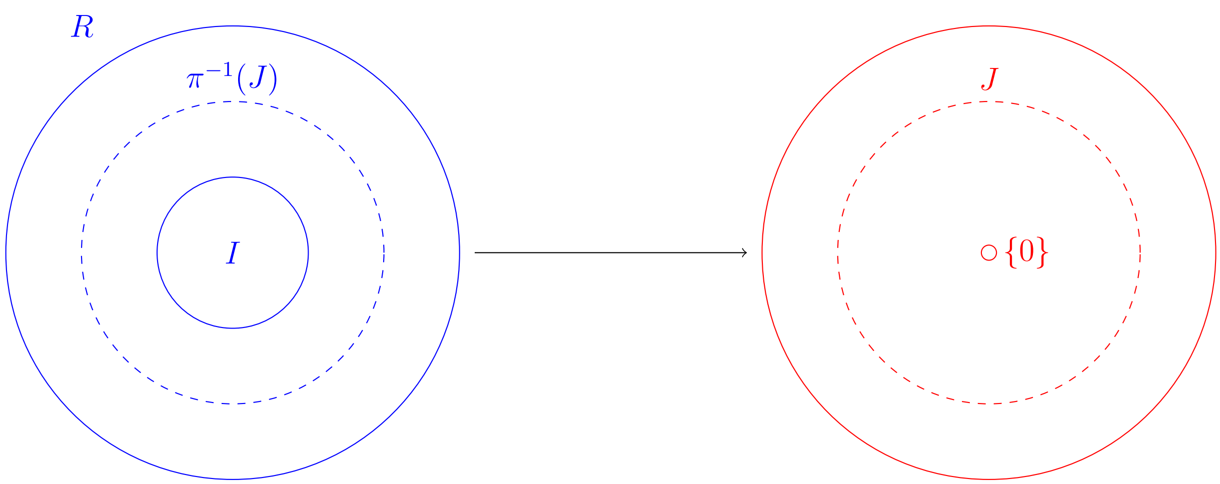
$$1 = ap + bn$$

$ap \in J$ because $ap \in p\mathbb{Z} \subset J$ and $bn \in J$ by absorber. Thus $1 \in J$ so $J = (1) = \mathbb{Z}$.

Lecture 11: Oct 17

Setup: R is a commutative ring and I is an ideal of R. We have a quotient ring $R/I = \{a+I \mid a \in R\}$ and a map $\pi : R \to R/I$ defined by $\pi(a) = a+I = \{a+b \mid b-I\}$

R



Meadow: a ring whose only ideals are (0) and R; synonymous with field

Lemma: there is an isomorphism between

$$\overset{A}{\{\text{Ideals of } R \text{ which contain } I\}} \iff \overset{B}{\{\text{Ideals of } R/I\}}$$

Proof: To show there is an isomorphism between A and B it suffices to show that there are maps $f : A \to B$ and $g : B \to A$ where $f^{-1} = g$.

Take an element $K \in A$. Then $\pi(K)$ is a member of B and we just need to check that $\pi(K)$ is an ideal of R/I. Conversely, if $J \in B$, we need to check $\pi^{-1}(J)$ is an ideal of R.

Finally, we just need to check that the functions π and π^{-1} are in fact inverses:

$$\begin{cases} \pi(\pi^{-1}(J)) = J \\ \pi^{-1}(\pi(K)) = K \end{cases}$$

1. Show $\pi(K)$ is an ideal:

$$\begin{aligned} \pi(0) = 0 &\implies 0 \in \pi(K) \\ \pi(a) + \pi(b) =& \pi(a+b) \in \pi(K) & (\pi(a), \pi(b) \in \pi(K) \forall a, b \in K) \\ -\pi(a) =& \pi(-a) \in \pi(K) & (\pi \text{ is homomorphism and } -a \in K) \\ r\pi(a) = \pi(c)\pi(a) =& \pi(ca) \in \pi(K) & (r \in R/I \implies r = \pi(c) \mid c \in R) \end{aligned}$$

2. Show $\pi^{-1}(J)$ is an ideal: (Basically same proof)

3. Show $\pi(\pi^{-1}(J)) = J$:

   By definition of π^{-1}, $\pi(\pi^{-1}(J)) \subset J$. Then we want show that $J \subset \pi(\pi^{-1}(J))$. Pick $a \in J$. Since π is onto, $a = \pi(r),\ r \in R$. Because $\pi(r) \in J$, $r \in \pi^{-1}(J)$. So $a = \pi(r) \in \pi(\pi^{-1}(J))$

4. Show $\pi^{-1}(\pi(K)) = K$:

   First we show $K \subset \pi^{-1}(\pi(K))$. Pick $a \in K$. Then $\pi(a) \in \pi(K) \implies a \in \pi^{-1}(\pi(k))$ because a has the property that it is mapped into $\pi(K)$ by π.

   To show $\pi^{-1}(\pi(K)) \subset K$, choose $a \in \pi^{-1}(\pi(K))$. We know $\pi(a) \in \pi(K)$ so $\pi(a) = \pi(b) \mid b \in K$ so $\pi(a) - \pi(b) = \pi(a-b) = 0 \implies a-b \in I \implies a-b \in K$ (because $I \subset K$). So $a = (a-b) + b \in K$.

Fields

Lecture 12: Oct 19

Review

There is a bijective map between the set of ideals of R that contain I and the ideals of R/I given a homomorphism $\pi : R \to R/I$

Theorems:

- R/I is an integral domain if and only if I is a prime ideal
- R/I is a field if and only if I is maximal

Defining Fields

A field is:

- A ring where every non-zero element has an inverse
- A ring whose only ideals are R and $\{0\}$
- The quotient R/I if and only if I is maximal
- A ring with division and commutativity

Example of Fields:

- $\mathbb{Q}$ - the rational numbers
- $\mathbb{R}$ - the real numbers

- $\mathbb{C}$ - complex numbers ($x + yi \mid x, y \in \mathbb{R}$ i.e., the set of linear combinations of x and i)
- $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ (*Proof:* $(a + b\sqrt{2})(a - b\sqrt{2}) = a - 2b^2$)
- $\mathbb{Q}[\sqrt{D}]$ (if D is not a perfect square)
- $\mathbb{Z}/p\mathbb{Z}$ if P is prime (because $p\mathbb{Z}$ is maximal)
- $F = \{a + b \diamond \mid a, b \in \mathbb{Z}/3\} = \mathbb{Z}/3[x]/(x^2 - 2)\mathbb{Z}/3[x]$ where $\diamond^2 = 2$ in $\mathbb{Z}/3$ (this set has 9 elements because a and b each have three values)

Interlude: Constructing the rational numbers

$$\mathbb{Q} = a \star b, b \neq 0, a_1 \star b_1 \sim a_2 \star b_2 \iff a_1 b_2 = a_2 b_1$$

with multiplication defined on the equivalence class of quotients

$$[a_1 \star b_1][a_2 \star b_2] = [a_1 a_2 \star b_1 b_2]$$

and addition defined

$$[a_1 \star b_1] + [a_2 \star b_2] = [a_1 b_2 + a_2 b_1 \star b_1 b_2]$$

Note that $\star$ is an operation that functions exactly like division but is meant to emphasize that it carries no other intrinsic properties except these operations on equivalence classes.

Vector spaces

Definition: a set V is a *vector space* over a field $\mathbb{F}$ if

1. V is an abelian group (under addition)
2. $(a + b)\vec{v} = a\vec{v} + b\vec{v} \quad \forall a, b \in \mathbb{F}, \vec{v} \in V$
3. $(ab)\vec{v} = a(b\vec{v}) \quad \forall a, b \in \mathbb{F}, \vec{v} \in V$
4. $a(\vec{w} + \vec{w}) = a\vec{v} + a\vec{w} \quad \forall a \in \mathbb{F}, \vec{v}, \vec{w} \in V$

Examples:

- $\mathbb{R}^n$
- $\mathbb{C}^n$

- $\mathbb{Q}^n$
- (Extension Field) Given fields $\mathbb{F} \subset K$, K (the extension field) is a vector space over $\mathbb{F}$ (the subfield)
- $\mathbb{C}$ is a vector space over $\mathbb{R}$
- $\mathbb{R}$ is a vector space over $\mathbb{Q}$
- $\mathbb{Q}[\sqrt{2}]$ is a vector space over $\mathbb{Q}$
- $\mathbb{Z}/\mathbb{Z}[\diamond]$ is a vector space over $\mathbb{Z}/3\mathbb{Z}$

Linear combinations of $v_1, v_2, \ldots,\ v_n \in V$:

$$sum_{i=1}^{n} a_i v_i \quad a_i \in \mathbb{F}$$

Spanning set: $\{v_i\}$ is a spanning set if every $v \in V$ is a linear combo of $\{v_i\}$

Independent set: $\{v_i\}$ is an independent set if

$$\sum_{i=1}^{n} a_i v_i = 0 \implies a_1, \ldots,\ a_n = 0$$

Basis: $\{v_i\}$ is a basis if it is an independent spanning set

Theorem: If V has a finite basis, then all bases have the same number of elements (which we call $\dim(V)$)

Axiom of Choice: postulate that every vector space has a basis

Lecture 13: Oct 24

Notation: $F[x]$ is ring set of polynomials with coefficients in F

Long division of polynomials

Theorem: (Division Algorithm)

Suppose you have two polynomials

$$p(x) = a_m x^m + \cdots + a_1, \quad a_i \in F, a_m \neq 0$$
$$q(x) = b_n x^n + \cdots + b_1, \quad b_i \in F, b_n \neq 0$$

(We say $\deg(p) = m$ and $\deg(q) = n$)

Then $q(x) = a(x)p(x) + r(x)$ where $\deg(r) < \deg(p)$

Proof: Induction on $n - m$

Base case: $n - m < 0$ so $q = 0p + r$

Generally,

$$q_* = q - \frac{b_n}{a_m} x^{n-m} p(x) \qquad \deg(q_*) = n_* < n$$

By induction,

$$q_* = a_* p + r \qquad \deg(r) < \deg(p)$$

so

$$q - \frac{b_n}{a_m} x^{n-m} p(x) = a_* p + r \implies q = \underbrace{(a_* + \frac{b_n}{a_m} x^{n-m})}_{a} p + r \quad \blacksquare$$

Theorems of Polynomial Rings

Theorem: All ideals in $F[x]$ are principal

Proof: Let I be an ideal. Consider $p(x) \in I$, the smallest degree non-zero polynomial in I. Let $q \neq 0 \in I$. By the division algorithm,

$$q = ap + r \quad \deg r < \deg p$$

Since $r = q - ap$, and I is ideal, $r \in I$. Therefore, $\deg r = 0$ (or else it would be smaller than p). Thus, $q = ap$ which is a contradiction.

Definition: $p(x) \in F[x]$ is *irreducible* if $p(x) = a(x)b(x) \implies \deg(a) = 0 \vee \deg(b) = 0$

Theorem: if $p(x) \in F[x]$ is irreducible, then $I = p(x)F[x]$ is maximal

Proof: Let $J = b(x)F[x]$ be an ideal such that $I \subseteq J \subseteq F[x]$. We know $p \in J$ because $p \in I$. So

$$p(x) = a(x)b(x)$$

Case 1: $\deg(a) = 0$ so $p = b$ up to constants and $I = J$

Case 2: $\deg(b) = 0$ so $1 \in J \implies J = F[x]$ (because inverse of $b \in F[x]$)

Theorem: $F[x]/p(x)F[x]$ is a field.

Proof: Given $c \in F$, consider the coset $[c] = c + p(x)q(x)$. We define a ring homomorphism $\phi : F \to F/p(x)F[x], c \mapsto [c]$.

Suppose $c \in \ker \phi$. Then

$$[c] = [0] \implies c \in p(x)F[x] \implies c = a(x)p(x) \implies a(x) = c \implies c = 0$$

So $\ker \phi = 0$. Then by the isomorphism theorem, F is isomorphic to $\phi(F)$ which means that $\phi(F)$ is a field.

Theorem: $F[x]/p(x)F[x]$ contains a root of $p(x)$

Proof: Consider $[x] = x + p(x)F[x]$. Since $\phi(F)$ contains a copy of F (mapped to its cosets), we can write

$$p([x]) = [p(x)] = [0]$$

by using the formula for coset composition.

Lecture 14: Oct 26

Review

Polynomial division: we can write any polynomial $q = ap + r$ where $\deg r < \deg p$

Theorems:

- if F is a field, all ideals in $F[x]$ are principal
- If $p \in F[x]$ is irreducible, then $I = p(x)F[x]$ is maximal
- $F[x]/p(x)F[x]$ is a field (look at the map $\phi : F \to F[x]/p(x)F[x], \quad a \mapsto [a] = a + p(x)F[x]$)
- $F[x]/p(x)F[x]$ contains a root of $p(x)$

  Proof:

$$p(x) = a_0 + \cdots + a_n x^n \in F[x]$$
$$p(x) = [a_0] + \cdots + [a_n]x^2 \in K[x]$$
$$p([x]) = [a_0] + \cdots + [a_n][x]^2 = [a_0 + a_1 x + \ldots a_n x^b] = [p(x)] = [0] \in K$$

An Example: $F = \mathbb{R}, \quad p(x) = x^2 + 1, \quad K = R[x]/(x^2+1)R[x]$ We know $x^2 + 1$ is irreducible because $\sqrt{-1} \notin \mathbb{R}$. We then consider the map $r \to [r]$ so

$$[x]^2 + [1] = 0 \tag{9}$$
$$[x]^2 = [-1] \tag{10}$$

We define $i := [x]$ so $i^2 = -1$. Further,

$$[x] + i[y] \in K$$

for amy element in k because

$$[x^n] = [x^2][x^{n-2}] = [-x^{n-2}]$$

so we can factor down any polynomial to lowest degree.

Bases

Basis: a linearly independent spanning set

Example: $\{1, i\}$ is a basis of $\mathbb{C}$ over $\mathbb{R}$

Example: Is $S = \{[1], [x], \ldots,\ [x^{n-1}]\}$ a basis? *Proof:* It is a spanning set because

$$[x^n] = -\frac{[a_{n-1}][x^{n-1}]}{[a_n]} \cdot -\frac{[a_0]}{[a_n]}$$

Suppose it is not linearly independent. then $\exists [b_0], \ldots,\ [b_{n-1}]$ such that

$$[b_0][x] + \cdots + [b_{n-1}][x^{n-1}] = [0]$$

Using the formula,

$$[b_0 + \cdots + b_{n-1}x^{n-1}] = [0] = [p(x)]$$

Since the polynomial is in the ideal, it is a multiple of $p(x)$. But p has degree n and $\deg([b_0 + \cdots + b_{n-1}x^{n-1}]) = n - 1$. But since $n - 1 < n$, it cannot be a multiple of p so contradiction.

Dimensionality

Let $\subset K$. Then we denote

$$[K : F] = \dim_F K = \text{the dimension of K as a vector space over F}$$

Example: $[\mathbb{C} : \mathbb{R}] = 2$ (because the basis is $\{1, i\}$)

Example: $[F[x]/p(x)F[x] : F] = \deg(p)$

A Homework Problem: $F = \mathbb{Q},\ p(x) = x^3 - 2$

$$[F[x]/F[x](x^3 - 2) : \mathbb{Q}] = 3$$

(Here $[x] = \sqrt[3]{2}$) and the basis is

$$\{[1], [x], [x^2]\} = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$$

Theorem: $F \subset K \subset L$,

$$[L : F] = [L : K][K : F]$$

Proof: Let $m = [K : F], \quad n = [L : K]$. Let $v_1, \ldots,\ v_m$ be an F-basis for K. Let $w_1, \ldots,\ w_n$ be a K-basis for L. We consider the set $\{v_i w_j\}$ and seek to prove that it is a spanning set and linearly independent.

Lemma: $\{v_i w_j\}$ is a spanning set.

Proof: Pick an element $l \in L$. It can be written in the form

$$l = \sum_i \sum_j k_{ij} v_i w_j$$

Lemma: $\{v_i w_j\}$ is independent

Proof: Suppose $\sum_{i,j} f_{ij} v_i w_j = 0$.

$$\left(\sum_i f_{i1} v_i\right) w_1 + \cdots + \left(\sum_i f_{in} v_i\right) w_n = 0$$

But the v_i are a basis for K so

$$\sum_{i,j} f_{ij} v_i = 0 \implies f_{ij} = 0 \quad \blacksquare$$