THE ALGEBRAIC GEOMETRY ALGEBRAIC TOPOLOGY DUMP

ERNEST YEUNG ERNESTYALUMNI@GMAIL.COM

From the beginning of 2016, I decided to cease all explicit crowdfunding for any of my materials on physics, math. I failed to raise *any* funds from previous crowdfunding efforts. I decided that if I was going to live in *abundance*, I must lose a scarcity attitude. I am committed to keeping all of my material **open-sourced**. I give all my stuff *for free*.

In the beginning of 2017, I received a very generous donation from a reader from Norway who found these notes useful, through *PayPal*. If you find these notes useful, feel free to donate directly and easily through PayPal, which won't go through a 3rd. party such as indiegogo, kickstarter, patreon. Otherwise, under the *open-source MIT license*, feel free to copy, edit, paste, make your own versions, share, use as you wish.

gmail : ernestyalumni
linkedin : ernestyalumni
twitter : ernestyalumni

Contents

Date: 5 mars 2017.
Key words and phrases. Algebraic Geometry, Algebraic Topology.

ABSTRACT. Everything about Algebraic Geometry, Algebraic Topology

Part 1. Algebra; Groups, Rings, R-Modules, Categories

We should know some algebra. I will follow mostly Rotman (2010) [14].

1. Prime numbers, GCD (greatest common denominator), integers, Euler's totient, Chinese Remainder Theorem, integer divison, modulus, remainders; Euclid's Lemma

Definition 1 (natural numbers $\mathbb{N}$). *natural numbers* $\mathbb{N}$

$$\mathbb{N} = \{ \text{ integers } n | n \geq 0\} \tag{1}$$

i.e. $\mathbb{N}$ *is set of all nonnegative integers.*

Definition 2 (prime). *natural number* p *is* ***prime*** *if* $p \geq 2$*, and* $\nexists$ factorization $p = ab$*, where* $a < p$*,* $b < p$ *are natural numbers.*

Definition 3. $a, b \in \mathbb{Z}$ ***relatively prime*** *if* $\gcd(a, b) = 1$

Axiom 1. ***Least Integer Axiom*** $\exists$ *smallest integer in every* $C \subset \mathbb{N}$*,* $C \neq \emptyset$

cf. pp. 1, Ch. 1 Things Past of Rotman (2010) [14]

Theorem 1 (**Division Algorithm**)**.** $\forall a, b \in \mathbb{Z}$*,* $a \neq 0$*,* $\exists ! q, r \in \mathbb{Z}$ *s.t.*

$$b = qa + r \text{ and } 0 \leq r < |a|$$

Proof. Consider $n \in \mathbb{Z}$, $b - na \in \mathbb{Z}$
Let $C = \{ b - na | n \in \mathbb{Z}\} \bigcap \mathbb{N}$.
$C \neq \emptyset$ (otherwise, consider $b - na < 0$, $b < na$, then contradiction)
By Least Integer Axiom, $\exists$ smallest $r \in C$, $r = b - na$.
define $q = n$ when $r = b - na$.
Suppose

$$\begin{aligned} & qa + r = q'a + r' \\ & (q - q')a = r' - r \\ & |(q - q')a| = |r' - r| \end{aligned},$$

$0 \leq r' < |a|$. Now $0 \leq |r' - r| < |a|$
if $|q - q'| \neq 0$, $|(q - q')a| \geq |a|$

$$\Longrightarrow q = q', r = r'$$

Conclude both sides are 0 (by contradiction) □

cf. pp. 2, Thm. 1.4, Ch. 1 Things Past of Rotman (2010) [14]

Definition 4 (divisor)**.** $a, b \in \mathbb{Z}$*,* a ***divisor*** *of* b *if* $\exists d \in \mathbb{Z}$ *s.t.* $b = ad$*.*
a ***divides*** b *or* b *multiple of* a*, denote*

$$a | b$$

$a|b$ *iff* b *has remainder* $r = 0$ *after dividing by* a

cf. pp. 3, Ch. 1 Things Past of Rotman (2010) [14]

1.1. Greatest Common Denominator (GCD); Euclid's Lemma.

Definition 5 (common divisor)**.** ***common divisor*** *of integers* a *and* b*, is integer* c*, s.t.* $c|a$ and $c|b$.
greatest common divisor *or* ***gcd*** *of* a *and* b*, denoted* $(a, b) \equiv gcd(a, b)$ *defined by*

$$(a, b) \equiv gcd(a, b) = \begin{cases} 0 & \text{if } a = 0 = b \\ & \text{the largest common divisor of } a \text{ and } b \text{ otherwise} \end{cases}$$

cf. pp. 3, Ch. 1 Things Past of Rotman (2010) [14]

Theorem 2. *If* $a, b \in \mathbb{Z}$*, then* $gcd(a, b) \equiv (a, b) = d$ *is linear combination of* a *and* b*, i.e.* $\exists s, t \in \mathbb{Z}$ *s.t.*

$$d = sa + tb \tag{2}$$

cf. pp.4, Thm. 1.7, Ch. 1 Things Past of Rotman (2010) [14]

Proof. Let $I :=$

$$I := \{ sa + tb | s, t \in \mathbb{Z}\}$$

If $I \neq \{0\}$, let d be smallest positive integer in I.
$d \in I$, so $d = sa + tb$ for some $s, t \in \mathbb{Z}$.
Claim: $I = (d) \equiv \{ kd | k \in \mathbb{Z}\}$ = set of all multiples of d.
Clearly $(d) \subseteq I$, since $kd = k(sa + tb) = (ks)a + (kt)b \in I$.
Let $c \in I$.
By division algorithm, $c = qd + r$, $0 \leq r < d$

$$r = c - qd = s'a + t'b - qsa - qtb = (s' - sq)a + (t' - qt)b \in I$$

If $r \in I$, but $r < d$, contradiction that $\min_{\substack{i \in I \\ i > 0}} i = d$.
So $r = 0$, and $d|c = c/d$.

$$c \in (d), \text{ so } I \subseteq (d) \Longrightarrow I = (d)$$

□

Theorem 3 (**Euclid's Lemma**; 1.10 of Rotman (2010) [14])**.** *If* p *prime and* $p|ab$*, then* $p|a$ *or* $p|b$*.*
More generally,
if prime p *divides product* $a_1 a_2 \ldots a_n$*,*
then it must divide at least 1 of the factors a_i*.*
i.e. (notation),
If prime p*, and* $ab/p \in \mathbb{Z}$*,*
then $a/p \in \mathbb{Z}$ *or* $b/p \in \mathbb{Z}$*.*
More generally,
if prime p*, s.t.* $a_1 a_2 \ldots a_n / p \in \mathbb{Z}$*,*
then $\exists$ *1* a_i *s.t.* $a_i/p \in \mathbb{Z}$

Proof. If $p \nmid a$, i.e. $a/p \notin \mathbb{Z}$, then $\gcd(p, a) \equiv (p, a) = 1$.
From Thm. 2,

$$1 = sp + ta$$
$$\Longrightarrow b = spb + tab = p(sb + td)$$

ab/p and so $ab = pd$, so $b = spb + tdp$, i.e. b is a multiple of p ($b/p \in \mathbb{Z} \equiv p|b$). □

Corollary 1 (1.11 of Rotman (2010) [14])**.** *Let* $a, b, c \in \mathbb{Z}$*.*
If c, a *relatively prime, i.e.* $gcd(c, a) = 1$*, and if* $c|ab \equiv ab/c \in \mathbb{Z}$*, then* $c|b \equiv b/c \in \mathbb{Z}$

Proof.

$$\gcd(c, a) = 1 = sc + ta \Longrightarrow b = sbc + tab = sbc + t(qc) = c(sb + tq) \Longrightarrow b/c = sb + tq$$

□

Theorem 4 (Euclidean Algorithm). *Let $a, b \in \mathbb{Z}^+$.*
$\exists$ algorithm that finds $d = \gcd a, b$

cf. pp. 5, Thm. 1.14 (Euclidean Algorithm), Ch. 1 Things Past of Rotman (2010) [14].

Proof. □

Definition 6. *Let fixed $m \geq 0$. Then $a, b \in \mathbb{Z}$ are* ***congruent modulo*** *m, denoted by*

$$a \equiv b \bmod m$$

if $m|(a-b)$, i.e. $(a-b)/m \in \mathbb{Z}$, i.e. if $(a-b)/m \in \mathbb{Z}$, i.e. $(a-b)$ integer multiple of m

Proposition 1. *If $m \geq 0$ is fixed, $m \in \mathbb{Z}$, then $\forall a, b, c \in \mathbb{Z}$*

(1) $a \equiv a \bmod m$
(2) *if $a \equiv b \bmod m$, then $b \equiv a \bmod m$*
(3) *if $a \equiv b \bmod m$, and $b \equiv c \bmod m$, then $a \equiv c \bmod m$*

cf. Prop. 1.18 of Rotman (2010) [14]

Proof. (1) $(a-a)/m = 0/m = 0$
(2) $(b-a)/m = (-1)(a-b)/m \in \mathbb{Z}$
(3) $(a-c)/m = (a-b+b-c)/m = (a-b)/m + (b-c)/m \in \mathbb{Z}$ □

EY : 20171225 to recap,

$$\boxed{\begin{gathered} a \equiv b \bmod n \\ \text{meaning} \\ \frac{a-b}{n} \in \mathbb{Z} \text{ or } a-b = kn,\ k \in \mathbb{Z} \text{ or } a = b + kN \text{ but rather} \\ a = pn + r \\ b = qn + r \end{gathered}} \qquad (3)$$

for $a = b + kn$, but b need not be a remainder of division of a by n. More precisely, $a = b \bmod n$ asserts that a, b have the same remainder when divided by n, i.e.

$$a = pn + r$$
$$b = qn + r$$

So $a \sim b$ or $[a] = [b]$ is an equivalence relation since
$a \sim a$ since $a \equiv a \bmod N$, since $a = a + 0N$,
if $a \sim b$, then $b \sim a$, since $a - b = kN$, then $b = a - kN$

if $a \sim b$, $b \sim c$, then $a \sim c$, since $\begin{aligned} a - b &= kN \\ b - c &= lN \end{aligned}$, then $a - c = (k+l)N$.

cf. Prop. 1.19 of Rotman (2010) [14]

Proposition 2. *Let $m \geq 0$ be fixed*

(1) *If $a = qm + r$, then $a \equiv r \bmod m$*
(2) *If $0 \leq r' < r < m$, then $r \not\equiv \bmod m$ i.e. r and r' aren't congruent $\bmod m$*
(3) *$a \equiv b \bmod m$ iff a, b leave same remainder after dividing by m*
(4) *If $m \geq 2$, $\forall a \in \mathbb{Z}$, $a \equiv b \bmod m$ for some $b \in 0, 1, \dots m-1$*

Proof. (1) If $a = qm + r$, then $a \equiv r \bmod m$

$$\frac{a-r}{m} = q \in \mathbb{Z}$$

(2) *Want*: If $0 \leq r' < r < m$, then $r \not\equiv \bmod m$.
Suppose $\frac{r-r'}{m} = k \in \mathbb{Z}$. Then $r - r' = km$ or $r = r' + km$.

$$m > r > r' \leq 0$$
$$m > r' + km > r' \leq 0$$
$$m - r' > km > 0$$

But $k > 0$ (since $m > 0$ and $r - r' = km > 0$) and $m - r' > km > 0$ is a contradiction.

(3) *Want*: $a \equiv b \bmod m$ iff a, b leave same remainder after dividing by m. By
By Division Algorithm, this is true:

$$a = q_a m + r_a$$
$$b = q_b m + r_b$$
$$\frac{a-b}{m} = q_a + \frac{r_a}{m} - q_b - \frac{r_b}{m} = k = q_a - q_b + \frac{r_a - r_b}{m} \in \mathbb{Z}$$

Now

$$|m| > r_a \leq 0$$
$$|m| > r_b \leq 0$$

$2|m| > r_a + r_b$.
And if $r_a > r_b$, $|m| > r_a > r_a - r_b > 0$.
In both cases, $r_a = r_b$ since $q_a - q_b + \frac{r_a - r_b}{m} \in \mathbb{Z}$ needs to be enforced.

(4) *Want*: If $m \geq 2$, $\forall a \in \mathbb{Z}$, $a \equiv b \bmod m$ for some $b \in 0, 1, \dots m-1$.
By Division Algorithm, $a = q_a m + r_a$, $0 \leq r_a < |m|$. $\frac{a - r_a}{m} = q_a \in \mathbb{Z}$ so let $b = r_a$. □

Theorem 5 (1.26 of Rotman (2010) [14]). *If $gcd(a, m) \equiv (a, m) = 1$, then $\forall b \in \mathbb{Z}$, $\exists x$ s.t.*

$$ax \equiv b \bmod m$$

In fact, $x = sb$, where $sa \equiv 1 \bmod m$ is 1 solution. Moreover, any 2 solutions are congruent $\bmod m$.
i.e.
If $\gcd a, b = 1$, then $\forall y \in \mathbb{Z}$, $\exists x$ s.t. $ax \equiv y \bmod b$, $x = sy$, where $sa \equiv 1 \bmod b$ is 1 solution. Moreover, any 2 solutions are congruent $\bmod m$. *This implies that*

$ax \equiv y \bmod b$ or $\frac{Ax - y}{b} \in \mathbb{Z}$, and $\frac{(as-1)y}{b} \in \mathbb{Z}$.
$sa \equiv 1 \bmod b$ or $\frac{sa-1}{b} \in \mathbb{Z}$, which implies that $sa - 1 = b(-t)$ or

$$sa + tb = 1$$

for some $s, t \in \mathbb{Z}$.

Proof. $\gcd(a, m) = 1 = sa + tm$, by Thm. 2
Then $b = b \cdot 1 = b(sa + tm) = sab + tmb$ or $b = tbm + sab$ or $a(sb) = -tbm + b$.
So $a(sb) \bmod m \equiv b$.
Let $x := sb$ and so $ax \bmod m = b$.
Now suppose $x \neq sb$ s.t. $ax \bmod m = b$. Then $ax = qm + b$. From $a(sb) \bmod m = b$, we also get $a(sb) = q'm + b$. Then $a(x - sb) \bmod m = 0$, so $m|a(x - sb) \equiv a(x - sb)/m \in \mathbb{Z}$.
By Corollary 1 (which says, if $\gcd(c, a) = 1$ and if $ab/c \in \mathbb{Z}$, then $b/c \in \mathbb{Z}$), since $\gcd(m, a) = (m, a) = 1$, and since $a(x - sb)/m \in \mathbb{Z}$, then $(x - sb)/m \in \mathbb{Z}$. So $(x - sb) = qm$ or $(sb) \bmod m = x$. □

Proposition 3 (3.1 of Scheinerman (2006) [15])**.** *Let $a, b \in \mathbb{Z}$, let $c = a \bmod b$, i.e. $a = qb + c$ s.t. $0 \leq c < b$.*
Then

$$gcd(a, b) = gcd(b, c) \tag{4}$$

cf. Sec. 3.3 Euclid's method of Scheinerman (2006) [15]

Proof. If d common divisor of a, b, i.e. $a/d, b/d \in \mathbb{Z} \equiv d|a, d|b$.
$c/d \in \mathbb{Z} \equiv d|c$ since $c = a - qb$.
If d is common divisor of b, c, i.e. $d|b, d|c \equiv c/d, b/d \in \mathbb{Z}$,
then $d|a \equiv a/d \in \mathbb{Z}$ since $a = qb + c$. So set of common divisors of a, b same as set of common divisors of b and c.
Then $\gcd(a, b) = \gcd(b, c)$. □

1.2. **Euler's totient; relatively prime.** cf. Ch. 5 Arrays, Sec. 5.1 Euler's totient of Scheinerman (2006) [15]
For

$$\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$$
$$\varphi : n \mapsto \varphi(n) := \text{ number of elements of } \{1, 2, \dots n\}$$

that are relative prime to

$$n = |\{i | i \in \{1, 2, \dots n\}, (n, i) = 1 \text{ or equivalently } n \propto i\}|$$

e.g. $\varphi(10) = 4$ since $\varphi(10) = |\{1, 3, 7, 9\}|$.
we want $|(a, b)| 1 \leq a, b, \leq n, \gcd(a, b) \equiv (a, b) = 1|$.

$$p_n = \frac{1}{n^2}\left[-1 + 2\sum_{i=1}^n \varphi(k)\right] =$$

$$= \text{ probability that 2 integers, chosen uniformly and independently from } \{1, 2, \dots n\} \text{ are relatively prime}$$

If p is prime, $\forall\, i \in \{1, 2, \dots p\}$, $(p, i) \equiv \gcd(p, i) = 1$, i.e. relatively prime to p, except 1 $i \in \{1, 2, \dots p\}$.
Therefore

$$\varphi(p) = p - 1$$

Consider $\varphi(p^2)$.
$\{1, 2, \dots p^2\}$, only numbers *not* relatively prime to p^2 are multiples of p since
$p, 2p, 3p, \dots p^2$ all divide p^2, i.e. $p|p^2, 2p|p^2 \dots (p-1)p|p^2 \equiv p^2/p, p^2/2p, \dots p^2/p(1-p)$.
Assume $\varphi(p^n) = p^2 - p^{n-1} = p^{n-1}(p-1)$.

$$\varphi(p^{n+1}) = \varphi(pp^n) = p^n\varphi(p) = p^n(p-1)$$

Therefore,

Proposition 4 (5.1)**.** *Let p prime, $n \in \mathbb{Z}^+$*

e.g. $\varphi(77)$.
$\forall\, n$ s.t. $1 \leq n \leq 77$.

$$\gcd(n, 77) = 1$$
$$\gcd(n, 7) = 1$$
$$\gcd(n, 11) = 1$$

By Prop. 3,

$$\gcd(n, 7) = \gcd(7, n \mod 7)$$
$$\gcd(n, 11) = \gcd(11, n \mod 11)$$

cf. Example (10) of Dummit and Foote [2].
To recap,

Definition 7 (Euler φ-function)**.** $\forall\, n \in \mathbb{Z}^+$,
let $\varphi(n) :=$ number of positive integers $a \leq n$ with a relatively prime to n, i.e. $\gcd(a, n) = 1 \equiv (a, n)$

e.g. $\varphi(12) = 4$, since $1, 5, 7, 11$ are only positive integers less than or equal to 12.
If p prime, $\varphi(p) = p - 1$.
More generally,
$\forall\, a \geq 1$,

$$\boxed{\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)} \tag{5}$$

φ is multiplicative in the sense that

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ if } \gcd(a, b) = 1 \tag{6}$$

$\Longrightarrow$ general formula.
If $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ (Fumdanetal Thm. of Arithmetic, $\forall\, n \in \mathbb{Z}, n > 1$), then

$$\boxed{\begin{aligned} &\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_s^{\alpha_s}) \\ &\quad p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_s^{\alpha_s - 1}(p_s - 1) \end{aligned}} \tag{7}$$

cf. pp. 69 Thm. 5.4 (Chinese Remainder) of Scheinerman (2006) [15].

Theorem 6. *Let $n \in \mathbb{Z}^+$,*
let $p_1, p_2, \dots p_t$ be distinct prime divisors of n (i.e. $\forall\, p_i$, $\frac{n}{p_i^{k_i}} \in \mathbb{Z}$ for some $k_i \geq 1$)
Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_t}\right) \tag{8}$$

Proof. By Fundamental Thm. of Arithmetic,

$$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$$

where p_j are distinct primes, and e_j are positive integers.
From Eqns. 5, 6, i.e. where

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$$
$$\varphi(ab) = \varphi(a)\varphi(b) \text{ if } \gcd(a, b) = 1$$
$$\varphi(n) = \varphi(p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \dots \varphi(p_t^{e_t}) =$$
$$= p_1^{e_1}(1 - \frac{1}{p_1})p_2^{e_2}(1 - \frac{1}{p_2}) \dots p_t^{e_t}(1 - \frac{1}{p_t}) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_t})$$

□

Exercise 10. cf. pp. 7 Exercise 10 Dummit and Foote [2].
Prove: $\forall$ given $N \in \mathbb{Z}^+$ (positive number),
$\exists$ only finite many integers n with $\varphi(n) = N$, where φ denotes Euler's φ-function.
EY, Indeed, by definition,

$$\varphi(n) = N$$
$$a_1, a_2 \dots a_N \text{ s.t. } a_i \leq n$$
$$\gcd(a_i, n) = 1 \text{ i.e. } 1 = s_i a_i + t_i n$$

Given $N \in \mathbb{Z}^+$, let $n \in \mathbb{Z}$, s.t. $\varphi(n) = N$ (given hypothesis).
Let $p =$ least (i.e. smallest) prime s.t. $p > N + 1$.
If $q \geq p$ is a prime divisor of n, i.e.

$$n = q^k m$$

for some $k \geq 1$, and m with q not dividing m.

Then

$$\varphi(n) = \varphi(q^k)\varphi(m) = q^{k-1}(q-1)\varphi(m) \geq q-1 \geq p-1 > N$$

Contradiction.

Thus, $\nexists$ prime divisor of n greater than $N+1$.

Particularly, distinct prime divisors of n belong to a finite set, say these primes are $p_1, p_2 \dots p_m$.

Definition 8. *prime divisor q of n if q is prime and*

$$\frac{n}{q} \in \mathbb{Z} \text{ i.e. } n = q^k m \text{ for some } k \geq 1 \text{ and } \frac{m}{q} \notin \mathbb{Z}^+ \quad (9)$$

Now

$$n = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$$

for some $0 < a_i$, so

$$\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})\dots\varphi(p_m^{a_m}), \text{ so } \varphi(n) = \prod_{i=1}^m p_i^{a_i-1}(p_i - 1)$$

Note, $\forall$ prime p_i, $\varphi(n) \geq p_i^{a_i-1}(p_i-1) \geq p_i - 1 > N$ for sufficiently large a_i.

Thus, $\forall p_i$, $\exists$ only finitely many permissible choices for exponents a_i.

So set of all n with $\varphi(n) = N$ is subset of finite set, hence finite.

$\forall N \in \mathbb{Z}^+$, $\exists$ largest integer n with $\varphi(n) = N$.

Thus, as $n \to \infty$, $\varphi(n) \to \infty$.

Scheinerman (2006) [15]

cf. Ex. 1.19, pp. 13, Sec. 1.1 Some Number Theory of Rotman (2010) [14] **Exercise 1.19.** If a and b are relatively prime and if each divides an integer n, then their product ab also divides n, i.e.

Theorem 7. *If $\gcd a, b = 1$, and if $n/a \in \mathbb{Z} \equiv a|n$, and $n/b \in \mathbb{Z} \equiv b|n$, then $n/ab \in \mathbb{Z} \equiv ab|n$.*

Proof. $\gcd a, b = 1$, so $sa + tb = 1$ for some $s, t \in \mathbb{Z}$ (Thm. 5).

$\frac{n}{a}, \frac{n}{b} \in \mathbb{Z}$, so $n = au$, $n = bv$

$n = n \cdot 1 = n(sa + tb) = bvsa + autb = ab(vs + ut)$, so $\frac{n}{ab} = vs + ut \in \mathbb{Z}$. □

1.2.1. *Chinese Remainder Theorem.*

Theorem 8. *If m, m' relatively prime (i.e. $\gcd(m, m') = 1$), then for*

$$x \equiv b \bmod m$$
$$x \equiv b' \bmod m'$$

i.e. given $b, b'm, m'$, and wanting to find x, $\exists x$ and $\forall 2x$'s, $x = x' \mod mm'$, i.e.

Let m, n relatively prime positive integers (i.e. $\gcd m, n = 1$),
$\forall a, b \in \mathbb{Z}$,
then pair of congruences
$x \equiv a \bmod m$
$x \equiv b \bmod n$
has a solution (x), and this solution x is uniquely determined, modulo mn.

Proof. cf. The Chinese Remainder Theorem by Keith Conrad

Suppose
$(x-a)/m \in \mathbb{Z}$ or $x - a = my$
$(x-b)/n \in \mathbb{Z}$ or $x - b = nz$ or $a + my - b = nz$
$\gcd m, n = 1$, so then $\forall b \in \mathbb{Z}$, $\exists w$ s.t. $mw \equiv b \bmod n$ i.e. $\frac{mw-b}{n} \in \mathbb{Z}$, in fact, $w = sb$, where $sm \equiv 1 \bmod n$, or $\frac{sm-1}{n} \in \mathbb{Z}$, is 1 solution (Thm. 5).

$$my = b - a + nz$$
$$smy = sb - sa + snz = (1 + nv)y = s(b-a) + snz \text{ or } y = s(b-a) + n(sz - vy)$$
$$\text{or } y \equiv s(b-a) \bmod n$$

$$x = a + my = a + m(s(b-a) + n(sz - vy)) = a + ms(b-a) + mn(sz - vy) \equiv a + ms(b-a) + mnu$$
$$x - a = m(s(b-a) + nu) \Longrightarrow x = a \bmod m$$
$$x - b = a + ms(b-a) + mnu - b = a + (1+m)(b-a) + mnu - b = m(b-a) + mnu \Longrightarrow x \equiv b \bmod n$$

Uniqueness: Suppose $x, y \in \mathbb{Z}$ s.t.

$$x \equiv a \bmod m \qquad y \equiv a \bmod m$$
$$x \equiv b \bmod n \qquad y \equiv b \bmod n$$

Given $\gcd m, n = 1$, $sm + tn = 1$.

Since $\frac{x-a}{m}, \frac{y-a}{m} \in \mathbb{Z}$, $\frac{x-y}{m} \in \mathbb{Z}$, likewise, $\frac{x-a}{n}, \frac{y-a}{n} \in \mathbb{Z}$, $\frac{x-y}{n} \in \mathbb{Z}$

Since $\frac{x-y}{m}, \frac{x-y}{n} \in \mathbb{Z}$, $\frac{x-y}{mn} \in \mathbb{Z}$ by Thm. 7.

Thus, $x - y = mnk$ for some $k \in \mathbb{Z}$. For instance, $k = 0$, $x = y$.

This shows any 2 solutions are the same, modulo mn. □

cf. Ch. 1 Things Past, Thm. 1.28 of Rotman (2010) [14], pp. 68 Thm. 5.2 (Chinese Remainder) of Scheinerman (2006) [15].

2. Groups

cf. pp. 16 Chapter 1 Introduction to Groups. Dummit and Foote (2004) [2]

Definition 9 (binary operation)**.** (1) *binary operation $*$ on set G is a function $* : G \times G \to G$. $\forall a, b \in G$, $a * b \equiv *(a, b)$*
(2) *binary operation $*$ on set G is* associative*: if $\forall a, b, c \in G$, $a * (b * c) = (a * b) * c$*
(3) *If $*$ is binary operation on set G, a, b of G commut if $a * b = b * a$.*
$*$ (or G) is ***commutative*** *if $\forall a, b \in G$ $a * b = b * a$.*

cf. pp. 16. Sec. 1.1. Basic Axioms and Examples, Dummit and Foote (2004) [2]

Definition 10 (Group)**.** (1) *Group is an ordered pair $(G, *)$ where G is a set, $*$ is a binary operation on G s.t.*
(a) $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$, *i.e.* $*$ associative
(b) $\exists e \in G$, *s.t.* $\forall a \in G$, $a * e = e * a = a$ *($\exists$* identity *e)*
(c) $\forall a \in G$, $\exists a^{-1} \in G$, *called an* inverse *of a, s.t. $a * a^{-1} = a^{-1} * a = e$*
(2) *(optional; abelian or* commutative*) $(G, *)$ abelian (or commutative) if $a * b = b * a$, $\forall a, b \in G$.*

e.g.
(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups under $+$ with $e = 0$ and $a^{-1} = -a$, $\forall a$.
(2) $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Q}^+, \mathbb{R}^+$ groups under $\times$ with $e = 1$, $a^{-1} = \frac{1}{a}$
(3) (**direct product of groups**)If $(A, *), (B, \circ)$ are groups, we can form new group $A \times B$ called **direct product** s.t.

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

and $(a_1, b_1)(a_2, b_2) = (a_1 * a_2, b_1 \circ b_2)$ cf. Example 6, Sec. 1.1 Dummit and Foote (2004) [2]

Proposition 5. *If G group under operation $*$, then*
(1) *identity of G is unique*
(2) *$\forall a \in G$, a^{-1} uniquely determined.*
(3) *$(a^{-1})^{-1} = a \quad \forall a \in G$*
(4) *$(a * b)^{-1} = (b^{-1}) * (a^{-1})$*
(5) *$\forall a_1, a_2, \dots a_n \in G$, $a_1, a_2 \dots a_n$ independent of how expression is bracketed (generalized associative law)*

cf. Prop. 1, Sec. 1.1 Dummit and Foote (2004)[2]

3. Groups; normal subgroups

Definition 11 (normal subgroup $K \lhd G$)**.**
normal subgroup *K of $G \equiv K \lhd G$ -*
subgroup $K \subset G$, if $\forall\, k \in K$, $\forall\, g \in G$,

$$gkg^{-1} \in K$$

Definition 12 (quotient group)**.**
quotient group *$G \mod K \equiv G/K$ -*
if G/K = family of all left cosets of subgroups $K \subset G =$

$$= \{gK | g \in G, K = \{gk | k \in K\}$$

and
K = normal subgroup of G, i.e. $K \lhd G$, and so

$$aKbK = abK \qquad \forall\, a, b \in G,$$

so G/K group.

Definition 13 (exact sequence of groups)**.** ***exact sequence*** *if $imf_{n+1} = kerf_n \qquad \forall\, n$ for sequence of group homomorphisms and groups*

$$G_{n+1} \xrightarrow{f_{n+1}} G_n \xrightarrow{f_n} G_{n-1} \tag{10}$$

Theorem 9. (1)

$$1 \qquad A \xrightarrow{f} B$$

(2)

$$B \xrightarrow{g} C \qquad 1$$

(3)

$$1 \qquad A \xrightarrow{h} B \qquad 1$$

Proof. (1) $\text{im}(1 \to A) = 1$, since $1 \to A$ is a group homomorphism ($(1 \to A)(1) = 1_A$).
if $1 \to A \overset{f}{\mapsto} B$ exact, $\ker f = \text{im}(1 \to A) = 1$, so if $f(x) = 1$, $x = 1$, f injective.
If f injective, $\ker f = 1$. $1 = \text{im}(1 \to A)$. $1 \to A \overset{f}{\mapsto} B$, exact.
(2) $\ker(C \to 1) = C$, by def. of $C \to 1$
if $B \overset{g}{\mapsto} C \to 1$ exact, $\text{im} g = g(B) = \ker(C \to 1) = C$. $g(B) = C$ implies g surjective.
If g surjective, $g(B) = C = \ker(C \to 1)$. $B \overset{g}{\mapsto} C \to 1$ exact.
(3) From (i), $1 \to A \overset{h}{\mapsto} B$ exact iff h injective. From (ii), $A \overset{h}{\mapsto} B \to 1$, exact iff h surjective.
h isomorphism. □

3.1. 1st, 2nd, 3rd Isomorphism Theorems.

Theorem 10 (1st Isomorphism Theorem (Modules) Thm. 7.8 of Rotman (2010) [14])**.** *If $f : M \to N$ is R-map of modules, then $\exists\, R$-isomorphism s.t.*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"] & N \\ M/kerf \arrow[ur, "\varphi =\cong"'] & \end{tikzcd}$$

$$\begin{aligned} & \varphi : M/kerf \to imf \\ & \varphi : m + kerf \mapsto f(m) \end{aligned} \tag{11}$$

Proof. View M, N as abelian groups.

Recall natural map $\pi : M \to M/N$
$m \mapsto m + N$
Define φ s.t. $\varphi\pi = f$.
(φ well-defined). Let $m + \ker f = m' + \ker f$, $m, m' \in M$, then $\exists\, n \in \ker f$ s.t. $m = m' + n$.

$$\varphi(m + \ker f) = \varphi\pi(m) = f(m) = f(m' + n) = f(m') + f(n) = \varphi\pi(m') + 0 = \varphi(m' + \ker f)$$

$\Longrightarrow \varphi$ well-defined.
(φ surjective). Clearly, $\text{im}\varphi \subseteq \text{im}f$.
Let $y \in \text{im}f$. So $\exists\, m \in M$ s.t. $y = f(m)$. $f(m) = \varphi\pi(m) = \varphi(m + \ker f) = y$. So $y \in \text{im}\varphi$. $\text{im}f \subseteq \text{im}\varphi$.
$\Longrightarrow \varphi$ surjective.
(φ injective) If $\varphi(a + \ker f) = \varphi(b + \ker f)$, then

$$\varphi\pi(a) = \varphi\pi(b) \text{ or } f(a) = f(b) \text{ or } 0 = f(a) - f(b) = f(a - b) \text{ so } a - b \in \ker f (a - b) + \ker f = \ker f \text{ so } a + \ker f = b + \ker f$$

φ isomorphism.
φ R-map. $\varphi(r(m + N)) = \varphi(rm + N) = f(rm)$.
Since f R-map, $f(rm) = rf(m) = r\varphi(m + N)$. φ is R-map indeed. □

Theorem 11 (2nd Isomorphism Theorem (Modules) Thm. 7.9 of Rotman (2011) [14])**.** *If S, T are submodules of module M, i.e. $S, T \in M$, then $\exists$ $R-$isomorphism*

$$\begin{tikzcd} S \arrow[r, "h"] \arrow[d, "\pi|_S"] & (S+T)/T = imh \\ S/(S \cap T) = S/kerh \arrow[ur, "\cong"'] & \end{tikzcd}$$

$$S/(S \cap T) \to (S + T)/T \tag{12}$$

Proof. Let natural map $\pi : M \to M/T$.
So $\ker\pi = T$.
Define $h := \pi|_S$, so $h : S \to M/T$, so $\ker h = S \cap T$,

$$(S + T)/T = \{(s + t) + T | a \in S + T, s \in S, t \in T\}$$

i.e. $(S + T)/T$ consists of all those cosets in M/T having a representation in S.
By 1st. isomorphism theorem,

$$S/S \cap T \xrightarrow{\cong} (S + T)/T$$

□

Theorem 12 (3rd Isomorphism Theorem (Modules) Thm. 7.10 of Rotman (2011) [14]). *If $T \subseteq S \subseteq M$ is a tower of submodules, then $\exists$ R-isomorphism*

$$\begin{tikzcd} M/T \arrow[r, "g"] \arrow[d, "\pi"] & M/S \\ (M/T)/(S/T) = (M/T)/\ker g \arrow[ur, "\cong"'] & \end{tikzcd}$$

$$(M/T)/(S/T) \to M/S \tag{13}$$

Proof. Define $g : M/T \to M/S$ to be **coset enlargement**, i.e.

$$g : M + T \mapsto m + S \tag{14}$$

g well-defined: if $m + T = m' + T$, then $m - m' \in T \subseteq S$, and $m + S = m' + S \Longrightarrow g(m + T) = g(m' + T)$

$\ker g = S/T$ since

$$\begin{aligned} g(s + T) &= s + S = S \qquad (S/T \subseteq \ker g) \\ g(m + T) &= m + S = 0 = S = s + S, \text{ so } m = s \Longrightarrow \ker g \subseteq S/T \end{aligned}$$

$\text{im} g = M/S$ since

$$\begin{aligned} g(m + T) &= m + S \Longrightarrow \text{ im} g \subseteq M/S \\ m + S &= g(m + T) \end{aligned}$$

Then by 1st isomorphism, and commutative diagram, done. ☐

4. Rings

Definition 14 (division ring). *ring R with identity 1, where $1 \neq 0$ is a **division ring** (or skew field) if $\forall a \in R$, $a \neq 0$, $\exists$ multiplicative inverse $1/a$, i.e. $\exists b \in R$ s.t. $ab = ba = 1$*

e.g.

(1) rational numbers $\mathbb{Q}$
real numbers $\mathbb{R}$
complex numbers $\mathbb{C}$
are commutative rings with identity (in fact, they're fields)
Ring axioms for each follow ultimately from ring axioms for $\mathbb{Z}$
(verified when $\mathbb{Z}$ constructed from $\mathbb{Z}$ (Sec. 7.5)), $\mathbb{C}$ from $\mathbb{R}$ (Example 1, Sec. 13.1).
Construction of $\mathbb{R}$ from $\mathbb{Z}$ carried out in basic analysis texts

(2) **quotient group** $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity (element 1) under operations of addition and multiplication of residue classes (frequently referred to as "modular arithmetic").
We saw additive abelian groups axioms followed from general principles of theory of quotient groups ($\mathbb{Z}/n\mathbb{Z}$) was prototypical quotient group. cf. Example 4, pp. 224, Dummit and Foote (2014)[2]

(3) **the (real) Hamiltonian Quaternions**.

Definition 15 ((real) Hamiltonian Quaternions). *Let $\mathbb{H} = \{a+bi+cj+dk | a, b, c, d \in \mathbb{R}\}$ s.t. "componentwise" addition is defined as*

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k \tag{15}$$

and multiplication defined by expanding using distributive laws

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k)$$

using

$$\begin{aligned} i^2 &= j^2 = k^2 = -1 \\ ij &= -ji = k \\ jk &= -kj = i \\ ki &= -ik = j \end{aligned} \tag{16}$$

Working out the multiplication

$$\begin{aligned} &(a + bi + cj + dk)(a' + b'i + c'j + d'k) = \\ &= \begin{matrix} aa' + ab'i + ac'j + ad'k + ba'i - bb' + bc'k - bd'j + \\ ca'j - cb'k - cc' + cd'i + da'k + db'j - dc'i - dd' = \end{matrix} \\ &= aa' - bb' - cc' - dd' + (ab' + ba' + cd' - dc')i + (ac' - bd' + ca' + db')j + (ad' + bc' - cb' + da')k \end{aligned}$$

Hamiltonian Quaternions are noncommutative ring with identity $(1 = 1 + 0i + 0j + 0k)$.
Similarly define *rational* Hamiltonian Quaternions ring by taking $a, b, c, d \in \mathbb{Q}$.
real and rational Hamiltonian Quaternions both are divison rings, where inverse of nonzero element defined as

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \tag{17}$$

cf. Example 5, pp. 224, Dummit and Foote (2014)[2]

(4) **rings of functions** (important class)
Let X be any nonempty set.
Let A be any ring.

Definition 16 (function ring). *collection $R = \{f : X \to A\}$ is a ring under pointwise addition and multiplication of functions s.t.*

$$\begin{aligned} (f + g)(x) &= f(x) + g(x) \\ (fg)(x) &= f(x)g(x) \end{aligned} \tag{18}$$

cf. Example 6, pp. 225, Dummit and Foote (2014)[2]

5. Commutative Rings

cf. Ch. 3 "Commutative Rings I" of Rotman (2010) [14]

Definition 17. *commutative ring R is a set with 2 binary operations, addition and multiplication, s.t.*

(i) *R abelian group under addition*
(ii) *(commutativity) $ab = ba \quad \forall a, b \in R$ (this isn't there for noncommutativity)*
(iii) *(associativity) $a(bc) = (ab)c \quad \forall a, b, c \in R$*
(iv) *$\exists 1 \in R$ s.t. $1a = a \quad \forall a \in R$ (many names used: one, unit, identity)*
(v) *(distributivity) $a(b + c) = ab + ac \quad a, b, c \in R$ (this splits up into 2 distributivity laws for noncommutativity)*

To reiterate, abelian group under addition R (is defined as)

(1) associative $\forall x, y, z \in R$, $x + (y + z) = (x + y) + z$
(2) $\exists 0 \in R$, $0 + x = x + 0$, $\forall x \in R$
(3) $\forall x \in R$, $\exists (-x) \in R$ s.t. $x + (-x) = 0 = (-x) + x$

abelian, if commutativity: $x + y = y + x$.

5.1. Linear Algebra; Linear Algebra with commutative rings as fields.

5.1.1. *Linear Algebra.*

Definition 18 (subspace)**.** *If V vector space over field k, then* ***subspace*** *of V is subset U of V s.t.*

(1) $0 \in U$
(2) $u, u' \in U$ *imply* $u + u' \in U$
(3) $u \in U$, *and* $a \in k$ *imply* $au \in U$

proper subspace *of* $V \equiv U \subsetneq V$ *is subspace* $U \subseteq V$ *with* $U \neq V$.

$U = V$, $U = \{0\}$ are always subspaces of a vector space V.
Examples (Example 3.70 Rotman (2010) [14])

(ii) If $V = (a_1, \dots a_n)$, $v \neq 0$, $v \in \mathbb{R}^n$,
line through origin $l = \{av | a \in \mathbb{R}\}$ is a subspace of $\mathbb{R}^n$.
plane through origin $= \{av_1 + bv_2 | v_1, v_2$ fixed pair of noncollinear vectors, $a, b \in \mathbb{R}\}$ are subspaces of $\mathbb{R}^n$
(iii) If $m \leq n$, $\mathbb{R}^m$ regarded as set of all vectors in $\mathbb{R}^n$ s.t. last $n - m$ coordinates are 0, then $\mathbb{R}^m$ subspace of $\mathbb{R}^n$. e.g. $\mathbb{R}^2 = \{(x, y, 0) \in \mathbb{R}^3\} \subsetneq \mathbb{R}^3$
(iv) If k field, **homogeneous linear system over** k of m equations in n unknowns is a set of equations

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= 0 \\ a_{21}x_1 + \dots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n &= 0 \end{aligned}$$

where $a_{ji} \in k$.
solution of this system is vector $(c_1 \dots c_n) \in k^n$ s.t. $\sum_i a_{ji}c_i = 0$, $\forall j$.
solution $(c_1 \dots c_n)$ **nontrivial** if $\exists$ some $c_i \neq 0$.
solution space (or null space) of system = set of all solutions.
solution space also a subspace of k^n

e.g. $k = \mathbb{I}_p$,

$$\begin{aligned} 3x - 2y + z &\equiv 1 \text{ mod } 7 \\ x + y - 2z &\equiv 0 \text{ mod } 7 \\ -x + 2y + z &\equiv 4 \text{ mod } 7 \end{aligned}$$

Definition 19 (list)**.** *list := vector space V is ordered set $v_1 \dots v_n$ of vectors in V, i.e. $\exists$ some $n \geq 1$, $\exists$ some function φ*

$$\varphi : \{1, 2 \dots n\} \to V$$

with $\varphi(i) = v_i \quad \forall i$

Thus, $X = \text{im}\varphi$.
X ordered, φ need not be injective.

Definition 20 (k-linear combination)**.** *k-linear combination of list $v_1 \dots v_n$ in V, $V \equiv$ vector space over field k, is vector v of form*

$$v = a_1v_1 + \dots + a_nv_n = \sum_{i=1} a_iv_i \quad \forall a_i \in k, \quad \forall i$$

Definition 21 (list)**.** *If list $X = v_1 \dots v_m$ in vector space V, then* ***subspace spanned by*** *X, $\langle v_1 \dots v_m \rangle :=$ set of all k-linear combinations of $v_1 \dots v_m$. Also, say $v_1 \dots v_m$ spans $\langle v_1 \dots v_m \rangle$.*

Lemma 1 ($\langle v_1 \dots v_m \rangle$ is smallest subspace of V containing $v_1 \dots v_m$)**.** (i) *Every intersection of subspaces of V is itself a subspace.*
(ii) *If $X = v_1 \dots v_m$ list in V, then intersection of all subspaces of V containing X is $\langle v_1 \dots v_m \rangle$, subspace spanned by $v_1 \dots v_m$, so $\langle v_1 \dots v_m \rangle$ is smallest subspace of V containing X.*

cf. (Lemma 3.71 Rotman (2010) [14])

Proof. (i) Consider $\bigcap_{\alpha \in I} V_\alpha$, $\forall \alpha \in I$, V_α subspace of V
(i) $0 \in V_\alpha$, $\forall \alpha \in I$, so $0 \in \bigcap_{\alpha \in I} V_\alpha$,
(ii) Let $u, u' \in \bigcap_{\alpha \in I} V_\alpha$. Then $u, u' \in V_\alpha$, $\forall \alpha \in I$. Consider $\beta \in I$. $u, u' \in V_\beta$, so $u + u' \in V_\beta$. Without loss of generality, $u + u' \in V_\alpha$, $\forall \alpha \in I$. Then $u + u' \in \bigcap_{\alpha \in I} V_\alpha$
(iii) Let $u \in \bigcap_{\alpha \in I} V_\alpha$. Consider $\alpha \in k$. Since $u \in V_\alpha$, $\forall \alpha \in I$, $au \in V_\alpha$, $\forall \alpha \in I$. Then $au \in \bigcap_{\alpha \in I} V_\alpha$
(ii) Let $X = \{v_1 \dots v_m\}$, let $\mathcal{S} \equiv$ family of all subspaces of V containing X.
$\bigcap_{S \in \mathcal{S}} S \subseteq \langle v_1 \dots v_m \rangle$ because $\langle v_1 \dots v_m \rangle \in \mathcal{S}$, since,
$\langle v_1 \dots v_m \rangle$ is *a* subspace of V containing X.
If $S \in \mathcal{S}$, then $S \ni v_1 \dots v_m$. As shown above, $\forall v \in \langle v_1 \dots v_m \rangle$, $v \in S$, and thus $v \in \bigcap_{S \in \mathcal{S}} S$. $\langle v_1 \dots v_m \rangle \subseteq \bigcap_{S \in \mathcal{S}} S$. □

Were all terminology in algebra consistent,
$\langle v_1 \dots v_m \rangle \equiv$ subspace *generated* by X.
Reason for different terms is that group theory, rings, vector spaces developed independently of each other.
Example 3.72 of Rotman (2010) [14]

(i)
(ii)
(iii) **polynomial vector space; polynomials as a vector space**.
Vector space need not be spanned by finite list.
e.g. $V = k[x]$,
Suppose $X = f_1(x) \dots f_m(x)$ finite list in V.
If $d =$ largest degree of any of $f_i(x)$,
then every (nonzero) k-linear combination of $f_1(x), \dots f_m(x)$ has degree at most d.
Thus $x^{d+1} \notin \langle f_1(x) \dots f_m(x) \rangle$, so X doesn't span $k[x]$

Definition 22 (finite-dimensional vector space; infinite-dimensional vector space)**.** *Vector space V is* ***finite-dimensional*** *if it's spanned by a finite list; otherwise V is* ***infinite-dimensional****.*

Proposition 6 (linear dependent span properties)**.** *If vector space V, list $X = v_! \dots v_m$ spanning V, following are equivalent:*

(i) *X isn't shortest spanning list*
(ii) *some v_i is in subspace spanned by others, i.e. $v_i \in \langle v_i \dots \widehat{v}_i \dots v_m \rangle$,*
(iii) *$\exists a_1 \dots a_m$ not all 0 s.t. $\sum_{l=1}^m a_l v_l = 0$*

Proof. (i) $\Longrightarrow$ (ii). If X isn't hosrtest spanning list, then 1 of vectors in X can be thrown out, and shorter list still spans, i.e. cf. Lemma 1(Lemma 3.71, Rotman (2010) [14]); let $\mathcal{S} \equiv$ family of all subspaces of V containing X.
EY: 20180610 Let $\bigcap_{S \in \mathcal{S}} S$. $\bigcap_{S \in \mathcal{S}} S \neq \langle v_1 \dots v_m \rangle$, $\bigcap_{S \in \mathcal{S}} S \subset \langle v_1 \dots v_m \rangle$
$\exists v \in \langle v_1 \dots v_m \rangle$, say$v = \sum_{i=1}^m a_i v_i$ s.t. $\exists S \in \mathcal{S}$, s.t. $v \notin S$.
(ii) $\Longrightarrow$ (iii) If $v_i = \sum_{j \neq i} c_j v_j$, define $a_i = -1 \neq 0$, $a_j = c_j$, $\forall j \neq i$. Then $\sum_{l=1}^m a_l v_l = -v_i + \sum_{j \neq i} c_j v_j = 0$
(iii) $\Longrightarrow$ (i) Suppose for $i \in 1 \dots m$, $a_i \neq 0$. $v_i = -\sum_{j \neq i} \frac{a_j}{a_i} v_j$. $\langle v_1 \dots \widehat{v}_i \dots v_m \rangle$ still spans V (i.e. deleting v_i gives a shorter list, which still spans).
For instance, if $v \in \langle v_1 \dots v_m \rangle$, $v = \sum_{l=1}$ □

Exercise 3.67. Suppose dim$V > 1$. Then $\exists$ at least 2 elements in a basis of V, say e_1, e_2. (Thm. 3.78 of Rotman (2010) [14], "Every finite-dim. vector space V has a basis; Def. of dim, "number of elements in a basis of V").

Consider subspaces $\langle e_1 \rangle$, $\langle e_2 \rangle$, subspaces spanned by e_1, e_2, respectively. Whether $V = \langle e_1, e_2 \rangle$ or $V = \langle e_1, e_2 \rangle$, $\langle e_1 \rangle, \langle e_2 \rangle \neq \{0\}$ nor V. Contradiction of hypothesis.

Thus, "If only subspaces of a vector space V are $\{0\}$ and V itself, $\dim(V) \leq 1$."

Proposition 7 (Matrix representation of linear transformation; 3.94 of Rotman (2010) [14]). *If linear transformation $T : k^n \to k^m$, then $\exists A \in Mat_k(m,n)$ s.t.*

$$T(y) = Ay, \qquad \forall y \in k^n$$

Proof. Let $\begin{matrix} (e_1 \dots e_n) & \text{standard basis of } k^n \\ (e_1' \dots e_m') & \text{standard basis of } k^m \end{matrix}$

Define $A = [a_{ij}]$, s.t. $T(e_j) = A_{*j} = A_{ij} e_i'$ (jth column),

If $\begin{matrix} S : k^n \to k^m \\ S(y) = A(y) \end{matrix}$, then

$$T(e_j) = a_{ij} e_i' = Ae_j$$

and so $\forall y = y_j e_j \in k^n$,

$$T(y) = T(y_j e_j) = y_j T(e_j) = y_j A_{ij} e_i' = Ay$$

$\square$

6. R-modules

cf. Sec. 7.1 Modules of Rotman (2010) [14]

Definition 23 (R-module). *R-module is (additive) abelian group M,*

equipped with scalar multiplication $\begin{aligned} R \times M &\to M \\ (r,m) &\mapsto rm \end{aligned}$

s.t. $\forall m, m' \in M$, $\forall r, r', 1 \in R$

(i) $r(m+m') = rm + rm'$
(ii) $(r+r')m = rm + r'm$
(iii) $(rr')m = r(r'm)$
(iv) $1m = m$

Example 7.1

(i) $\forall$ *vector space* over field k is a k-module. (by inspection of the axioms for a vector space, associativity, distributivity!)
(ii) $\forall$ abelian group is a $\mathbb{Z}$-module, by laws of exponents (Prop. 2.23)

Indeed, for

$$\begin{aligned} \mathbb{Z} \times M &\to M \\ (r,m) &\mapsto rm \equiv m^r \end{aligned}$$

and so

$$r(m \cdot m') \equiv (m \cdot m')^r = m^r (m')^r = rm + rm'$$

(since M abelian)

(iii) For commutative ring, scalar multiplication, defined to be given multiplication of elements of R

$$\begin{aligned} R \times R &\to R \\ (a,b) &\mapsto ab \end{aligned}$$

For reference, recall some of the properties of a commutative ring:

$$\begin{aligned} ab &= ba \\ a(bc) &= (ab)c \\ 1a &= a \\ a(b+c) &= ab + ac \end{aligned}$$

$\forall$ ideal I in R is an R-module,

for if $\begin{matrix} i \in I \\ r \in R \end{matrix}$, then $ri \in I$.

$0 \in I$

$\forall a, b \in I$, $a + b \in I$

If $a \in I$, $r \in R$, then $ra \in I$.

(iv)
(v) Let linear $T : V \to V$, V finite-dim. vector space over field k.

Recall $k[x] \equiv$ set of polynomials with coefficients in k.

Define $\begin{aligned} k[x] \times V &\to V \\ f(x)v &= \left(\sum_{i=0}^m c_i x^i \right) v = \sum_{i=0}^m c_i T^i(v) \end{aligned}$ $\quad \forall f(x) = \sum_{i=0}^m c_i x^i \in k[x]$

$\Longrightarrow$ denote $k[x]$-module V^T.

Special case: Let $A \in \mathrm{Mat}_k(n,n)$, let linear $\begin{matrix} T : k^n \to k^n. \\ T(w) = Aw \end{matrix}$

vector space k^n is $k[x]$-module if we define scalar multiplication

$$\begin{aligned} k[x] \times k^n &\to k^n \\ f(x)w &= \left(\sum_{i=0}^m c_i x^i \right) w = \sum_{i=0}^m c_i A^i w \end{aligned}$$

$\forall f(x) = \sum_{i=0}^m c_i x^i \in k[x]$

In $(k^n)^T$, $xw = T(w)$

In $(k^n)^A$, $xw = Ax$

$T(w) = Ax$ and so $(k^n)^T = (k^n)^A$ (EY : 20151015 because of induction?)

Definition 24 (R-homomorphism (or R-map)). *If ring R, R-modules M, N, then function $f : M \to N$, if $\forall m, m' \in M$, $\forall r \in R$,*

$$\begin{aligned} f(m+m') &= f(m) + f(m') \\ f(rm) &= rf(m) \end{aligned}$$

Example 7.2. of Rotman (2011) on pp. 425 [14]]

(i) If R field, then R-modules are vector spaces and R-maps are linear transformations. Isomorphisms are then nonsingular linear transformations.
(ii)
(iii)
(iv)
(v) Let linear $T : V \to V$, let $v_1 \dots v_n$ be basis of V, let A be matrix of T relative to this basis.

Let $e_1 \dots e_n$ be standard basis of k^n.

Define $\begin{aligned} \varphi &: V \to k^n \\ \varphi(v_i) &= e_i \end{aligned}$

$$\varphi(xv_i) = \varphi(T(v_i)) = \varphi(v_j a_{ji}) = a_{ji}\varphi(v_j) = a_{ji}e_j$$
$$x\varphi(v_i) = A\varphi(v_i) = Ae_i$$

$\implies \varphi(xv) = x\varphi(v) \quad \forall v \in V$

By induction on $\deg f$, $\varphi(f(x)v) = f(x)\varphi(v) \qquad \forall f(x) \in k[x] \qquad \forall v \in V$

$\implies \varphi$ is $k[x]$-map

$\implies \varphi$ is $k[x]$-isomorphism of V^T and $(k^n)^A$.

Proposition 8 (7.3 of Rotman (2011) [14])**.** *Let vector space over field k, V, let linear $T, S : V \to V$ Then $k[x]$-modules V^T, V^S are $k[x]$-isomorphic iff $\exists$ vector space isomorphism $\varphi : V \to V$ s.t. $S = \varphi T \varphi^{-1}$.*

Proof. If $\varphi : V^T \to V^S$is a $k[x]$-isomorphism,

$$\varphi(f(x)v) = f(x)\varphi(v) \quad \forall v \in V, \forall f(x) \in k[x]$$

if $f(x) = x$, then $\varphi(xv) = x\varphi(v)$

$$xv = T(v)$$
$$x\varphi(v) = S(\varphi(v))$$
$$\implies \varphi \circ T(v) = S \circ \varphi(v) \implies \varphi \circ T = S \circ \varphi$$

φ isomorphism, so $S = \varphi \circ T \circ \varphi^{-1}$

Conversely, if given isomorphism $\varphi : V \to V$ s.t. $S = \varphi T \varphi^{-1}$, then $S\varphi = \varphi T$.

$$S\varphi(v) = \varphi T(v) = \varphi(xv) = x\varphi(v)$$

Then by induction, $\varphi(x^n v) = x^n \varphi(v)$ (for $S^n \varphi(v) = x^n \varphi(v) = (\varphi T \varphi^{-1})^n \varphi(v) = \varphi T^n v = \varphi(x^n v)$).
By induction on $\deg(f)$, $\varphi(f(x)v) = f(x)\varphi(v)$. □

Corollary 2 (7.4 of Rotman (2011) [14])**.** *Let k be a field,*
Let $A, B \in Mat_k(n,n)$.
Then $k[x]$-modules $(k^n)^A$, $(k^n)^B$ are $k[x]$-isomorphic.
(recall, $k[x] \equiv$ set of polynomials with coefficients in $k = \{\sum_{i=0}^m c_i x^i | c_i \in k\}$, and define scalar multiplication

$$k[x] \times k^n \to k^n$$
$$f(x)w = \left(\sum_{i=0}^m c_i x^i \right) w = \sum_{i=0}^m c_i A^i w, \qquad \forall f(x) = \sum_{i=0}^m c_i x^i \in k[x]$$

)
iff $\exists$ nonsingular P with

$$B = PAP^{-1}$$

Proof. Define

$$\begin{aligned} T &: k^n \to k^n \\ T(y) &= A(y) \end{aligned}$$ where $y \in k^n$ is a column.

By Example 7.1 (v) of Rotman (2011) [14], recall,
and so for $k[x]$-module, $(k^n)^T = (k^n)^A$.
Similarly, define

$$S : k^n \to k^n$$
$$S(y) = B(y)$$

Denote corresponding $k[x]$-module by $(k^n)^B$.
Given $(k^n)^A \cong (k^n)^B$ (isomorphic), by Prop. 8,
$\exists$ isomorphism $\varphi : k^n \to k^n$ s.t. $B = \varphi A \varphi^{-1}$.

By Prop. 7, i.e. Prop. 3.94 of Rotman (2011) [14], in that every linear transformation has a matrix representation (even in the standard "Euclidean" basis), $\exists P \in \text{Mat}_k(n,n)$, s.t.

$$\varphi(y) = Py \qquad y \in k^n$$

(P nonsingular because φ isomorphism)
Thus,

$$B\varphi(y) = \varphi A(y)$$
$$BPy = P(Ay) \qquad \forall y \in k^n$$
$$\implies PA = BP \text{or } B = PAP^{-1}$$

Conversely, given $B = PAP^{-1}$, P nonsingular matrix,
define isomorphism

$$\varphi : k^n \to k^n$$
$$\varphi(y) = Py \qquad \forall y \in k^n$$

By Prop. 8,
$(k^n)^B$, $(k^n)^A$ are $k[x]$-isomorphic.
i.e. $\varphi : (k^n)^A \to (k^n)^B$ is a $k[x]$-module isomorphism. □

Definition 25 ($\text{Hom}_R(M,N)$)**.**
(19)
$$Hom_R(M,N) = \{ \text{ all } R\text{-homomorphisms } M \to N \} = \{ f | f : M \to N, \text{ s.t. } \forall m, m' \in M, \forall r \in R, \begin{matrix} f(m+m') = f(m) + f(m') \\ f(rm) = rf(m) \end{matrix} \}$$

If $f, g \in Hom_R(M,N)$,
define

$$\begin{aligned} f + g &: M \to N \\ f + g &: m \mapsto f(m) + g(m) \end{aligned} \tag{20}$$

Proposition 9 ($\text{Hom}_R(M,N)$ R-module, 7.5 of Rotman (2011) [14])**.** *If M, N R-modules, where R commutative ring, then $Hom_R(M,N)$ R-module,*
with addition

$$f + g : M \to N \qquad \forall f, g \in Hom_R(M,N)$$
$$f + g : m \mapsto f(m) + g(m)$$

and scalar multiplication

$$rf : m \mapsto f(rm)$$

Moreover, distributive laws:
If $p : M' \to M$, $q : N \to N'$, then

$$(f+g)p = fp + gp \text{ and } q(f+g) = qf + qg$$

$\forall f, g \in Hom_R(M,N)$

Proof. $\forall f, g \in \text{Hom}_R(M,N), \forall r, r', 1 \in R$,

(i)
$$r(f+g)(m) = (f+g)(rm) = f(rm) + g(rm) = rf(m) + rg(m) = (rf + rg)(m)$$

(ii)
$$(r+r')f(m) = f((r+r')m) = f(rm + r'm) = f(rm) + f(r'm) = (rf + r'f)(m)$$

(iii)
$$(rr')f(m) = f(rr'm) = rf(r'm) = f(r'rm) = f(rr'm) \implies (rr')f = r(r'f)$$

(iv)
$$1f(m) = f(1m) = f(m) \implies 1f = f$$

Definition 26. *if R-module M, the submodule N of M, denoted $N \subseteq M$, is additive subgroup N of M, closed under scalar multiplication $rn \in N$ whenever $n \in N$, $r \in R$*

Definition 27 (quotient module M/N)**.**
quotient module *M/N -*
For submodule N of R-module M, then, remember M abelian group, N subgroup, quotient group M/N equipped with scalar multiplication

$$r(m+N) = rm + N$$
$$M/N = \{m+N | m \in M\}$$

natural map

$$\begin{aligned} \pi : M &\to M/N \\ m &\mapsto m+N \end{aligned} \tag{21}$$

easily seen to be R-map.
Scalar multiplication in quotient module well-defined:
If $m+N = m'+N$, $m-m' \in N$, so $r(m-m') \in N$ (because N submodule), so

$$rm - rm' \in N \text{ and } rm + N = rm' + N$$

Proposition 10 (7.15 of Rotman (2010) [14])**.** (i) $S \bigsqcup T \simeq M$

(ii) $\exists$ *injective R-maps* $\begin{aligned} i : S \to M \\ j : T \to M \end{aligned}$, *s.t.*

$$\begin{gathered} M = im(i) + im(j) \text{ and} \\ im(i) \bigcap im(j) = \{0\} \end{gathered} \tag{22}$$

(iii) $\exists$ *R-maps*

$$\begin{aligned} i : S \to M \\ j : T \to M \end{aligned}$$

s.t. $\forall\, m \in M$, $\exists !$

$$\begin{aligned} s \in S \\ t \in T \end{aligned}$$

with $m = is + jt$.

(iv) $\exists$ *R-maps*

$$\begin{aligned} i : S \to M \qquad & p : M \to S \\ j : T \to M \qquad & q : M \to T \end{aligned}$$

s.t.

$$\begin{aligned} pi &= 1_S \\ qj &= 1_T \end{aligned} , \quad \begin{aligned} pj &= 0 \\ qi &= 0 \end{aligned} \quad ip + jq = 1_M$$

Proof.
- (i)$\to$ (ii) Given $S \bigsqcup T \simeq M$,
  let $\varphi : S \bigsqcup T \to M$ be this isomorphism.
  Define

  $$\begin{aligned} i &:= \varphi\lambda_S & (\lambda_S : s \mapsto (s,0)) && i : S \to M \\ j &:= \varphi\lambda_T & (\lambda_T : t \mapsto (0,t)) && j : T \to M \end{aligned}$$

  i, j are injections, being composites of injections.

  If $m \in M$, $\exists !\, (s,t) \in S \bigsqcup T$, s.t. $\varphi(s,t) = m$.
  Then

  $$m = \varphi(s,t) = \varphi((s,0)+(0,t)) = \varphi\lambda_S(s)\varphi\lambda_T(t) = is + jt \in \text{im}(i) + \text{im}(j)$$

  Let $c \in \text{im}(i) + \text{im}(j)$. Since $\begin{aligned} i : S \to M \\ j : T \to M \end{aligned}$, $c \in M$.
  $\Longrightarrow M = \text{im}(i) + \text{im}(j)$.
  If $x \in \text{im}(i) \bigcap \text{im}(j)$,

  $$\begin{aligned} x &= i(s) \text{ for some } s \in S \\ x &= j(t) \text{ for some } t \in T \end{aligned}$$

  $$is = jt = \varphi\lambda_S(s) = \varphi\lambda_T(t) = \varphi(s,0) = \varphi(0,t)$$

  φ isomorphism, so $\exists \varphi^{-1} \Longrightarrow (s,0) = (0,t)$, so $s = t = 0$. $x = 0$

- (ii)$\to$ (iii) Given $\begin{aligned} i : S \to M \\ j : T \to M \end{aligned}$, s.t. $M = \text{im}(i) + \text{im}(j)$, so
  $\forall\, m \in M$, $m = i(s) + j(t)$ for some $s \in S, t \in T$.

  Suppose $\begin{aligned} s' \in S \\ t' \in T \end{aligned}$, s.t. $m = i(s'_+ j(t')$.

  $$i(s-s') = j(t-t') \in \text{im}(i) \bigcap \text{im}(j) = \{0\}$$

  So $s = s', t = t'$, since i, j injective.
- (iii)$\to$ (iv)
  Given $\forall\, m \in M$, $\exists !\, s \in S, t \in T$ s.t.

  $$m = i(s) + j(t)$$

  Define

  $$\begin{aligned} p : M \to S \qquad & q : M \to T \\ p(m) := s \qquad & q(m) := t \end{aligned}$$

  $$\begin{aligned} pi(s) &= s \\ qj(t) &= t \end{aligned} \quad \begin{aligned} pj(t) &= 0 \\ qi(s) &= 0 \end{aligned} \quad (ip + jq)(m) = ip(m) + jq(m) = i(s) + j(t) = m$$

$\square$

7. Categories; Category Theory

7.1. **Categories.** cf. 7.2 Categories of Rotman (2010) [14]

7.1.1. *Russell paradox, Russell set.*

Definition 28 (Russell set)**.** *Russell set - set S that's not a member of itself, i.e. $S \notin R$*

If R is family of all Russell sets,
Let $X \in R$. Then $X \notin X$. But $X \in R$. $X \notin R$.
Let $R \notin R$. Then R in family of Russell Sets. $R \in R$. Contradiction.
Then consider *class* as primitive term, instead of set.

Definition 29 (Category)**.** *Category $\mathcal{C}$ (Rotman's notation) $\equiv$ $\mathbf{C}$ (my notation), consists of class obj$(\mathcal{C})$ (Rotman's notation) $\equiv Obj(\mathbf{C}) \equiv Obj\mathbf{C}$ (my notation) of objects, set of morphisms $Hom(A,B)$ $\forall (A,B)$ of ordered tuples of objects, composition*

$$\begin{gathered} Hom(A,B) \times Hom(B,C) \to Hom(A,C) \\ (f,g) \mapsto gf \end{gathered}$$

, s.t.

(1) $\exists \mathbf{1}, \forall f : A \to B, \exists \begin{aligned} 1_A &: A \to A \\ 1_B &: B \to B \end{aligned}$ *, s.t.* $1_B \cdot f = f = f \cdot 1_A$*, and*

(2) *associativity,* $\forall \begin{aligned} f &: A \to B \\ g &: B \to C \\ h &: C \to D \end{aligned}$*, then* $h \circ (g \circ f) = (h \circ g) \circ f$

In summary,

$$\mathbf{C} := (Obj(\mathbf{C}), Mor\mathbf{C}, \circ, \mathbf{1}) \equiv (Obj\mathbf{C}, Mor\mathbf{C}, \circ_{\mathbf{C}}, \mathbf{1}_{\mathbf{C}}) \tag{23}$$

s.t.

$$Mor\mathbf{C} = \bigcup_{A,B \in Obj\mathbf{C}} Hom(A,B)$$

Examples (7.25 of Rotman (2010)[14]):

(i) $\mathbf{C} = \text{Sets}$
(ii) $\mathbf{C} = \text{Groups} = \text{Grps}$
(iii) $\mathbf{C} = \text{CommRings}$
(iv) $\mathbf{C} = {}_R\mathbf{Mod}$, if $R = \mathbb{Z}$, ${}_\mathbb{Z}\mathbf{Mod} = \mathbf{Ab}$, i.e. $\mathbb{Z}-$modules are just abelian groups.
(v) $\mathbf{C} = \mathbf{PO}(X)$, If partially ordered set X, regard X as category, s.t. $\mathbf{Obj}, \mathbf{PO}(X) = \{ x | x \in X \}$, $\forall \text{Hom}(x,y) \in \mathbf{Mor}_{\mathbf{PO}}(X)$, $\text{Hom}(x,y) = \begin{cases} \emptyset & \text{if } x \not\preceq y \\ \kappa^x_y & \text{if } x \preceq y \end{cases}$ where $\kappa^x_y \equiv$ unique element in Hom set when $x \preceq y$) s.t.

$$\kappa^y_z \kappa^x_y = \kappa^x_z$$

Also, notice that

$$1_x = \kappa^x_x$$

Definition 30 (isormorphisms or equivalences)**.** *$f : A \to B$, $f \in Hom(A,B)$, if $\exists$ **inverse** $g : B \to A$, $g \in Hom(B,A)$, s.t.*

$$\begin{aligned} gf &= 1_A \\ fg &= 1_B \end{aligned}$$

*and if $\mathbf{C} =$ **Top**, equivalences (isomorphisms) are homeomorphisms.*

Feature of category ${}_R\mathbf{Mod}$ not shared by more general categories: *Homomorphisms can be added.*

Definition 31 (pre-additive Category)**.** *category* $\mathbf{C}$

We can force 2 overlapping subsets A, B to be disjoint by "disjointifying" them: e.g. consider $(A \cup B) \times \{1,2\}$, consider

$$\begin{aligned} A' &= A \times \{1\}. \\ B' &= B \times \{2\} \end{aligned}$$

$$\implies A' \cap B' = \emptyset$$

since $(a,1) \neq (b,2) \quad \forall a \in A, \forall b \in B$.

Let bijections $\begin{aligned} \alpha &: A \to A', \\ \beta &: B \to B' \end{aligned}$ $\quad \begin{aligned} \alpha &: a \mapsto (a,1), \\ \beta &: b \mapsto (b,2) \end{aligned}$ denote $A' \bigcup B' \equiv A \coprod B$.

From Rotman (2010) [14], pp. 447,

Definition 32. ***coproduct*** $A \coprod B \equiv C \in Obj(\mathcal{C})$

In my notation,
coproduct

$$\begin{aligned} &(\mu_1, A_1 \coprod A_2) \\ &(\mu_2, A_1 \coprod A_2) \end{aligned} \tag{24}$$

where injection (morphisms)

$$\begin{aligned} \mu_1 &: A_1 \to A_1 \coprod A_2 \\ \mu_2 &: A_1 \to A_1 \coprod A_2 \end{aligned} \tag{25}$$

s.t.

$$\forall A \in \text{Obj}\mathbf{A}, \forall f_1, f_2 \in \text{Mor}\mathbf{A} \text{ s.t. } \begin{aligned} f_1 &: A_1 \to A \\ f_2 &: A_2 \to A \end{aligned}$$

then

$$\begin{gathered} \exists ! [f_i] \equiv [f_1, f_2] \in \text{Mor}\mathbf{A}, [f_1, f_2] : A_1 \coprod A_2 \to A \text{ s.t.} \\ [f_1, f_2]\mu_1 = f_1 \\ [f_1, f_2]\mu_2 = f_2 \end{gathered} \tag{26}$$

i.e.

$$\begin{tikzcd}
 & A \\
A_1 \arrow[ur, "f_1"] \arrow[r, "\mu_1"] & A_1 \coprod A_2 \arrow[u, dashed, "{[f_1, f_2]}"'] \\
A_2 \arrow[uur, "f_2"] \arrow[ur, "\mu_2"'] &
\end{tikzcd} \tag{27}$$

So to generalized, for $i \in I$, (finite set I?)

coproduct $(\mu_j, \coprod_{i\in I} A_i)_{j\in I}$, where
(family of) injection (morphisms) $\mu_j : A_j \to \coprod_{i\in I} A_i$
s.t.

$$\forall\, A \in \text{Obj}\mathbf{A},\ \forall\, f_i \in \text{Mor}\mathbf{A},\ i \in I,\ f_i : A_i \to A$$

then

$$\exists!\, [f_i] \equiv [f_i]_{i\in I} \in \text{Mor}\mathbf{A},\ [f_i] : \coprod_{i\in I} A_i \to A \text{ s.t.} \tag{28}$$
$$[f_i]\mu_j = f_j \qquad \forall\, j \in I$$

i.e.

$$\begin{tikzcd} & A \\ A_j \arrow[ur, "f_j"] \arrow[r, "\mu_j"'] & \coprod_{i\in I} A_i \arrow[u, dashed, "{[f_i]}"'] \end{tikzcd} \tag{29}$$

For notation purposes only, recall that it's denoted the sets $\text{Hom}(A,B)$ in ${}_R\mathbf{Mod}$ by

$$\text{Hom}_R(A,B)$$

i.e., in my notation, for $A, B \in \text{Obj}_R\mathbf{Mod}$, $\text{Hom}(A,B) \subset \text{Mor}({}_R\mathbf{Mod})$, $\text{Hom}(A,B) \equiv \text{Hom}_R(A,B)$

Definition 33 (pre-additive category)**.** *category* $\mathbf{C}$ *is* ***pre-additive*** *if* $\forall\, Hom(A,B)$, $Hom(A,B)$ *equipped with binary operation* $+$ *s.t.* $\forall\, f, g \in Hom(A,B)$,

(1) *if* $p : B \to B'$, *then*
$$p(f+g) = pf + pg \in Hom(A, B')$$
(2) *if* $q : A' \to A$, *then*
$$(f+g)q = fq + gq \in Hom(A', B)$$

and
$$f + g = g + f \qquad \textit{(additive abelian)}$$

7.1.2. *Examples of extra assumptions on sets,* ${}_R$***Mod*** *we take for granted.* In Prop. 7.15(iii) Rotman (2010) [14],

$$\text{direct sum } M = A \oplus B \text{ if } \exists \text{ homomorphisms } \begin{matrix} p : M \to A \\ q : M \to B \\ i : A \to M \\ j : B \to M \end{matrix} \text{ s.t. } \begin{matrix} pi = 1_A \\ qj = 1_B, \\ pj = 0 \\ qi = 0 \end{matrix}$$
$$ip + jq = 1_M$$

direct sum $M = A \oplus B$ uses property that morphisms can be added ${}_R\mathbf{Mod}$ has this property. **Sets** don't.
In Corollary 7.17,
direct sum in terms of arrows,
$\exists$ map $\rho : M \to S$ s.t. $\rho(s) = s$. Moreover $\ker\rho = \text{im} j$, $\text{im}\rho = \text{im} i$ and $\rho(s) = s, \quad \forall\, s \in \text{im}\rho$.

$$\begin{tikzcd} S \arrow[r, "i"] & M & T \arrow[l, "j"'] \end{tikzcd} \quad \text{and } M \simeq S \coprod T,$$

where $i : s \mapsto s$ (i.e. inclusions)
$j : t \mapsto t$

This makes sense in **Sets**, but doesn't make sense in arbitrary categories because image of morphism may fail, e.g. $\text{Mor}(\mathcal{C}(G))$ are elements in $\text{Hom}(*,*) = G$, not functions.
Categorically, object S is (equivalent to) retract of object M, $S, M \in \text{Obj}\mathbf{C}$, if $\exists$ morphisms $i, p \in \text{Mor}(\mathbf{C})$, s.t.

$$i : S \to M$$
$$p : M \to S$$

s.t. $pi = 1_S$, $(ip)^2 = ip$ (for modules, define $\rho = ip$)

Definition 34 (free products)**.** ***free products*** *are coproducts in groups*

Prop. 7.26, Rotman (2010) [14]

Proposition 11 (7.26, Rotman)**.** *If* A, B *are R-modules,*
then their coproducts in ${}_R$***Mod*** *exists, and it's the direct sum* $C = A \coprod B$.

Proof. Define

$$\begin{matrix} \mu : A \to C \\ \mu : a \mapsto (a, c) \end{matrix} \qquad \begin{matrix} \nu : B \to C \\ \nu : b \mapsto (0, b) \end{matrix} \qquad \text{(Rotman's notation)} \begin{matrix} \alpha : A \to C \\ \beta : B \to C \end{matrix}$$

Let X be a module, $f : A \to X$, $g : B \to X$ homomorphisms ◻

Define
$$\theta : C \to X$$
$$\theta : (a,b) \mapsto f(a) + g(b)$$

$$\theta\mu(a) = \theta(a, 0) = f(a)$$
$$\theta\nu(b) = \theta(0, b) = g(b)$$

so diagram commutes, i.e.

$$\begin{tikzcd} & X & \\ A \arrow[ur, "f"] \arrow[r, "\mu"'] & C \arrow[u, dashed, "\theta"'] & B \arrow[ul, "g"'] \arrow[l, "\nu"] \end{tikzcd}$$

If $\psi : C \to X$ makes diagram commute,
$$\psi((a,0)) = f(a) \qquad \forall\, a \in A$$
$$\psi((0,b)) = g(b) \qquad \forall\, b \in B$$

and since ψ is a homomorphism, $\psi((a,b)) = \psi((a,0)) + \psi((0,b)) = f(a) + g(b) = \theta((a,b))$. $\psi = \theta$.
Prop. 7.27, Rotman (2010) [14]

Proposition 12 (7.27, Rotman)**.** *If category* $\mathcal{C} = \mathbf{C}$, *and if* $A, B \in Obj\mathbf{C}$, *then* $\forall$ *2 coproducts of* A, B, *if they* $\exists$, *are equivalent.*

Proof. Suppose C, D coproducts of A, B. Suppose coproducts $\begin{aligned} \mu_A &: A \to C, \qquad & \nu_A &: A \to D \\ \mu_B &: B \to C, \qquad & \nu_B &: B \to D \end{aligned}$

$$\begin{tikzcd} & D & \\ A \arrow[ur, "\nu_A"] \arrow[r, "\mu_A"] & C \arrow[u, dashed, "\theta"] & B \arrow[ul, "\nu_B"'] \arrow[l, "\mu_B"'] \end{tikzcd}$$

Just substitute $X = D$ in diagram above.
Then substitute again:

$$\begin{tikzcd} & C & \\ A \arrow[ur, "\mu_A"] \arrow[r, "\nu_A"] & D \arrow[u, dashed, "\psi"] & B \arrow[ul, "\mu_B"'] \arrow[l, "\nu_B"'] \end{tikzcd}$$

Then combine the 2 diagrams: $\psi\theta = 1_C$. Likewise by label symmetry of C, D, $\theta\psi = 1_D$.
Then C, D are equivalent. □

Exer. 7.29 on pp. 459 of Rotman (2010) [14]

Definition 35. *If $A, B \in Obj\mathbf{C}$, then their **product**; $A \prod B = P \in Obj\mathbf{C}$, and morphisms* $\begin{aligned} p &: P \to A \\ q &: P \to B \end{aligned}$ *s.t.* $\forall X \in Obj\mathbf{C}$,

$\forall\, f : X \to A \in Mor\mathbf{C}$,
$\quad g : X \to B \in Mor\mathbf{C}$
$\exists!\, \theta : X \to P$, *s.t.*

$$\begin{tikzcd} & X \arrow[dl, "f"'] \arrow[d, dashed, "\theta"] \arrow[dr, "g"] & \\ A & A \prod B \arrow[l, "p"'] \arrow[r, "q"] & B \end{tikzcd}$$

If the notation of Kashiwara and Schapira (2006) [1],

$$\begin{tikzcd} & Y \arrow[dl, "f_0"'] \arrow[d, dashed, "{[f_0 f_1]}"] \arrow[dr, "f_1"] & \\ X_0 & X_0 \prod X_1 \arrow[l, "p_0"'] \arrow[r, "p_1"] & X_1 \end{tikzcd}$$

In general

$$\begin{tikzcd} & Y \arrow[dl, "f_j"'] \arrow[d, dashed, "{[f_i]_{i\in I}}"] \\ X_j & \prod_{i \in I} X_i \arrow[l, "p_i"] \end{tikzcd}$$

***product** of X_i's,*

$$\prod_i X_i \equiv \prod_{i \in I} X_i$$

given by

$$\prod_i X_i := \varprojlim \alpha \qquad (30)$$

When $X_i = X$, $\forall\, i \in I$, denote product by $X^{\prod I} \equiv X^I$.

e.g. Cartesian product $P = A \times B$ of 2 sets A, B, $A, B \in \text{Obj}\mathbf{Sets}$.
Define

$$\begin{aligned} p &: A \times B \to A \qquad & q &: A \times B \to B \\ p(a,b) &\mapsto a & q(a,b) &\mapsto b \end{aligned}$$

If $X \in \text{Obj}\mathbf{Sets}$,

if $\begin{aligned} f &: X \to A, \\ g &: X \to B \end{aligned}$ then $\begin{aligned} \theta &: X \to A \times B \\ \theta &: x \mapsto (f(x), g(x)) \in A \times B \end{aligned}$

Proposition 13 (7.28 Rotman (2010); equivalence of products, if it exists)**.** *If $A, B \in Obj\mathbf{C}$, then $\forall$ 2 products of A and B, should they exist, are equivalent.*

Proof. Suppose C, D products of A, B. Suppose products $\begin{aligned} p_A &: C \to A, \qquad & q_A &: D \to A \\ p_B &: C \to B, \qquad & q_B &: D \to B \end{aligned}$

$$\begin{tikzcd} & D \arrow[dl, "q_A"'] \arrow[d, dashed, "\theta"] \arrow[dr, "q_B"] & \\ A & C \arrow[l, "p_A"'] \arrow[r, "p_B"] & B \end{tikzcd}$$

Just substitute $X = D$ in diagram above.

Then substitute again:

$$\begin{tikzcd} & C \arrow[dl, "p_A"'] \arrow[d, dashed, "\psi"] \arrow[dr, "p_B"] & \\ A & D \arrow[l, "q_A"'] \arrow[r, "q_B"] & B \end{tikzcd}$$

Then combine the 2 diagrams: $\psi\theta = 1_C$. Likewise by label symmetry of C, D, $\theta\psi = 1_D$.

Then C, D are equivalent. □

7.1.3. *Products of Modules and Sets.*

Proposition 14 (7.29 Rotman (2010); products of R-modules are equivalent)**.** *If commutative ring R, R-modules A, B, then $\exists$ their (categorical) product $A \sqcup B$, in fact*

$$A \sqcap B \cong A \sqcup B \tag{31}$$

Proof. If $A \sqcup B \cong M$, then $\exists$ R-maps, $\begin{matrix} i : S \to M, \\ j : T \to M \end{matrix}$ $\quad \begin{matrix} p : M \to S \\ q : M \to T \end{matrix}$ s.t. $\begin{matrix} pi = 1_A \\ qj = 1_B \end{matrix}$ and $\begin{matrix} pj = 0, \\ qi = 0 \end{matrix}$ and $ip + jq = 1_M$, i.e.

$$\begin{tikzcd} A \arrow[r, shift left, "i"] & M \arrow[l, shift left, "p"] \arrow[r, shift right, "q"'] & B \arrow[l, shift right, "j"'] \end{tikzcd}$$

If module X, since $\begin{matrix} f : X \to A \\ g : X \to B \end{matrix}$ are homomorphisms,

define $\begin{matrix} \theta : X \to A \sqcup B \\ \theta(x) = if(x) + jg(x) \end{matrix}$ so that

$$\begin{tikzcd} & X \arrow[dl, "f"'] \arrow[d, dashed, "\theta"] \arrow[dr, "g"] & \\ A & A\sqcup \arrow[l, "p"'] \arrow[r, "q"] & B \end{tikzcd}$$

since, $\forall x \in X$,

$$p\theta(x) = pif(x) + pjg(x) = pif(x) + 0 = f(x)$$

since $ip + jq = 1_{A \sqcup B}$

$$\psi = ip\psi + jq\psi = if + jf = \theta$$

so product is unique. □

Definition 36. *Let R be commutative ring, let $\{A_i : i \in I\}$ be indexed family of R-modules.*

direct product *$\prod_{i\in I} A_i$ is cartesian product (i.e. set of all I-tuples (a_i) whose ith coordinate a_i lies in A_i $\forall i$) with coordinate wise addition and scalar multiplication:*

$$\begin{aligned} (a_i) + (b_i) &= (a_i + b_i) \\ r(a_i) &= (ra_i) \end{aligned}$$

where $r \in R$, $a_i, b_i \in A_i$, $\forall i$

cf. Thm. 7.32 of Rotman (2010) [14]

Theorem 13 (7.32, Rotman)**.** *Let commutative ring R. $\forall$ R-module A, $\forall$ family $\{B_i | i \in I\}$ of R-modules,*

$$Hom_R(A, \coprod_{i\in I} B_i) \simeq \coprod_{i\in I} Hom_R(A, B_i) \tag{32}$$

via R-isomorphism

$$\varphi : f \mapsto (p_i f)$$

where p_i are projections of product $\coprod_{i\in I} B_i$

Proof. Let $a \in A$, $f, g \in \text{Hom}_R(A, \coprod_{i\in I} B_i)$.

$$\varphi(f+g)(a) = (p_i(f+g))(a) = (p_i(f(a) + g(a))) = (p_i f + p_i g)(a)$$

φ additive.

$\forall i$, $\forall r \in R$, $p_i r f = r p_i f$ (since product of R-modules, $\coprod_{i\in I} B_i$ is also an R-module of $\text{Obj}_R\mathbf{Mod}$, by def. of product).

$$\varphi r f \mapsto (p_i r f) = (r p_i f) = r(p_i f) = r\varphi(f)$$

So φ is R-map.

If $(f_i) \in \coprod_i \text{Hom}_R(A, B_i)$, then $f_i : A \to B_i$ $\forall i$

By Rotman's Prop. 7.31 (If family of R-modules $\{A_i | i \in I\}$, then direct product $C = \coprod_{i\in I} A_i$ is their product in ${}_R\mathbf{Mod}$),

By def. or product, $\exists!\, R$-map , $\theta : A \to \coprod_{i\in I} B_i$ s.t. $p_i\theta = f_i$ $\forall i$

$$\begin{tikzcd} & A \arrow[dl, "f_i"'] \arrow[d, dashed, "\theta"] \\ B_i & \prod_{i\in I} B_i \arrow[l, "p_i"] \end{tikzcd}$$

Then

$$f_i) = (p_i\theta) = \varphi(\theta)$$

, and so φ *surjective.*

Suppose $f \in \ker\varphi$, so $\theta = \varphi(f) = (p_i f)$. Thus $p_i f = 0$ $\forall i$

$$\begin{tikzcd} & A \arrow[dl, "0"'] \arrow[d, "f"] \\ B_i & \prod_{i\in I} B_i \arrow[l, "p_i"] \end{tikzcd}$$

But 0-homomorphism also makes this diagram commute, so uniqueness of homomorphism $A \to \prod B_i$ gives $f = 0$. □

8. Applications of Category Theory: Finite State Machines (FSM)

Definition 37 (Finite State Machines ≡ Finite State Automaton)**.** *A deterministic finite state machine or acceptor deterministic finite state machine is a quintuple* $(\Sigma, S, s_0, \delta F)$ *where*
$\Sigma \equiv$ *input alphabet (finite, non-empty set of symbols)*
$S \equiv$ *finite, non-empty set of states*
$s_0 \equiv$ *initial state,* $s_0 \in S$
$\delta \equiv$ *state-transition function;* $\delta : S \times \Sigma \to S$ *(in a nondeterministic finite automaton, it would be* $\delta : S \times \Sigma \to \mathcal{P}(S)$*), i.e.* δ *would return a set of states;* $\mathcal{P}(S) \equiv$ *set of all subsets of* S*, including* $\emptyset$ *and* $S \equiv$ *power set.*
$F \equiv$ *set of final states, (possibly empty subset of* S*;* $F \subseteq S$ *or* $F \subseteq S \cup \{\emptyset\}$*)*
Finite State Machine (FSM) is also known as a Finite State Automaton.

cf. Black, Paul E (12 May 2008). "Finite State Machine". *Dictionary of Algorithms and Data Structres*. U.S. National Institute of Standards and Technology (NIST).

For both deterministic and non-deterministic FSMs, it's conventional to allow δ to be a partial function, i.e. $\delta(q,x)$ doesn't have to be defined for every combination of $q \in S$, $x \in \Sigma$

If FSM M is in state q; the next symbol (input?) is x and $\delta(q,x)$ not defined; then M can announce an error (i.e. reject the input (???)).

Definition 38 (Alphabet)**.** *alphabet* $:=$ *nonempty set of symbols* $\equiv \Sigma$
string $:=$ *finite sequence of members (i.e. symbols) of an underlying base set (i.e.* ***alphabet****)*
$\Sigma^n \equiv$ *set of all strings of length* n*.*

Part 2. Category Theory

9. Note on notation

From the section on "Terminology" of the Preface of Barr and Wells (1998) [3]:

> "In most scientific disciplines, notation and terminology are standardized, of- ten by an international nomenclature committee. (Would you recognize Einstein's equation if it said $p = HU^2$?) We must warn the nonmathematician reader that such is not the case in mathematics. There is no standardization body and terminology and notation are individual and often idiosyncratic."

To try to bridge the difference choice of notation and through comparison, suggest the "best" notation that's easy to remember and easy to use, I'll present all the different types of notation that I come across as much as I can. My plan of attack is the following:

(1) I'll try to present different types of notation and reference the authors of the text when I can.
(2) I'll try to defer to the notation used in Wikipedia, first.
(3) I'll make a final decision of what notation works best (for me).

10. Category A, (definition)

Definition 39 (Category $\mathbf{A}$)**.** ***category*** $\mathbf{A}$ *is quadruple* $\mathbf{A} = (Obj(\mathbf{A}), Mor\mathbf{A}, 1, \circ)$

(33) $$\mathbf{A} = (Obj(\mathbf{A}), Mor\mathbf{A}, 1, \circ)$$

s.t.

(1) $Obj(\mathbf{A})$ *is a* class*, whose elements,* $A \in Obj(\mathbf{A})$*, are called* objects
(2) $Mor\mathbf{A}$ *is a* class.
  (a) *From Adámek, Herrlich, and Strecker (2004) [4], Kashiwara and Schapira (2006) [1],* $\forall A, B \in Obj(\mathbf{A})$*,* $\exists Hom(A,B) \subseteq Mor(\mathbf{A})$*. Therefore,*

(34) $$Mor\mathbf{A} = \bigcup_{A,B \in Obj(\mathbf{A})} Hom(A,B)$$

  (b) $\forall f \in Hom(A,B)$*,* $f : A \to B \in Hom(A,B)$ *is a* morphism.

$$A \xrightarrow{f} B$$

(3) $\forall A \in Obj(\mathbf{A})$*,* $\exists 1_A : A \to A$*, i.e.* $\exists \mathbf{1}_A \in Hom_{\mathbf{A}}(A,A) \equiv Hom(A,A)$*,*

$$\begin{tikzcd} A \arrow[r, "1_A"] & A \end{tikzcd} \quad or \quad \begin{tikzcd} A \arrow[loop left, "\mathbf{1}_A"] \end{tikzcd}$$

(4) ***composition:*** $\forall A, B, C \in Obj\mathbf{A}$*, define* ***composition*** *to be a map*

(35) $$\begin{aligned} Hom_{\mathbf{A}}(A,B) \times Hom_{\mathbf{A}}(B,C) &\to Hom_{\mathbf{A}}(A,C) \\ (f,g) &\mapsto g \circ f \end{aligned}$$

, i.e.

$\forall f : A \to B \in Hom(A,B)$*, i.e.* $f, g \in Mor\mathbf{A}$*,*
$g : B \to C \in Hom(B,C)$
then $g \circ f : A \to C \in Hom(A,C)$*,* $g \circ f \in Mor\mathbf{A}$ *i.e.*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

s.t.

  (a) associativity $\forall \begin{matrix} f : A \to B \\ g : B \to C \\ h : C \to D \end{matrix}$*,* $h \circ (g \circ f) = (h \circ g) \circ f$ *i.e.*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rrr, bend left, "(h \circ g) \circ f"] \arrow[rr, bend right, "g \circ f"'] \arrow[rrr, bend right=50, "h \circ (g \circ f)"'] & B \arrow[r, "g"] \arrow[rr, bend left, "h \circ g"] & C \arrow[r, "h"] & D \end{tikzcd}$$

  (b) $\forall f : A \to B \in Hom(A,B)$*,* $1_B \circ f = f$ *and* $f \circ 1_A = f$ *i.e.* $\forall f \in Hom_{\mathbf{A}}(A,B)$*,*

$$\begin{tikzcd} A \arrow[loop left, "1_A"] \arrow[r, "f"] & B \arrow[loop right, "1_B"] \end{tikzcd}$$

  (c) *Adámek, Herrlich, and Strecker (2004) [4] posited further that* $Hom(A,B) \in Mor\mathbf{A}$ *pairwise disjoint (i.e.* $Hom(A,B) \bigcap Hom(C,D) \neq \emptyset$ *if* $C \neq A$ *or* $D \neq B$*)*

10.1. **Examples.**

- **Set** $= (\text{Obj}(\mathbf{Set}), \text{Hom}\mathbf{Set}, \mathbf{1}, \circ)$ where
  Obj(**Set**) is the class of all sets
  Hom**Set** is the class of all functions on a set to another set
- **Vec**

$$\begin{aligned} \text{Obj}\mathbf{Vec} &\equiv \text{all real vector spaces} \\ \text{Mor}\mathbf{Vec} &\equiv \text{all linear transformations between them (between real vector spaces)} \end{aligned}$$

- **Monoid**. Consider a monoid as a triple $(M, \cdot, e)$.
  Every semigroup $(M, \cdot)$ (recall that a *semigroup* is a set S with binary operation $\cdot$, i.e. s.t.

$S \times S \xrightarrow{\cdot} S$
$\forall a, b, c \in S$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativity)
(but no inverse, necessarily!)) that also has a unit e can be made into a category $\mathbf{C}$
$\Longrightarrow \mathbf{C}(M, \cdot, e) = (\text{Obj}(\mathbf{C}), \text{Hom}(\mathbf{C}), \mathbf{1}, \circ)$, a category $\mathbf{C}$ with only 1 object, i.e. $\text{Obj}(\mathbf{C}) = \{M\}$, so that
$\text{Obj}(\mathbf{C}) = \{M\}$
$\text{Hom}(M, M) = M$
$\mathbf{1}_M = e$
$y \circ x = y \cdot x$

10.2. **Duality, opposite category.** Given a category $\mathbf{A} = (\text{Ob}, \text{hom}_{\mathbf{A}}, 1, \circ)$,

Definition 40 (dual opposite category)**.** ***dual*** *or* ***opposite*** *category of* $\mathbf{A} = (Obj(\mathbf{A}), Mor\mathbf{A}, \mathbf{1}, \circ)$, *denoted* $\mathbf{A}^{op}$, *is*

(36) $$\mathbf{A}^{op} = (Obj(\mathbf{A}), Mor\mathbf{A}^{op}, \mathbf{1}, \circ^{op})$$

s.t.

-

(37) $$Obj(\mathbf{A}^{op}) = Obj(\mathbf{A})$$

- $\forall A, B \in Obj(\mathbf{A}^{op})$, $Hom_{\mathbf{A}^{op}}(A, B) \subseteq Mor\mathbf{A}^{op}$,

(38) $$Hom_{\mathbf{A}^{op}}(A, B) = Hom_{\mathbf{A}}(B, A) \subseteq Mor\mathbf{A}$$

- Define *the new composition*

(39) $$\begin{aligned} f \circ^{op} g \;\; of \;\; g &\in Hom_{\mathbf{A}^{op}}(C, B) \\ f &\in Hom_{\mathbf{A}^{op}}(B, A) \\ &then \\ f \circ^{op} g &= g \circ f \end{aligned}$$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd} \qquad \textit{dual :} \qquad \begin{tikzcd} A & B \arrow[l, "f"'] & C \arrow[l, "g"'] \arrow[ll, bend left, "f \circ^{op} g"] \end{tikzcd}$$

or, equivalently (notation-wise)

$$\begin{tikzcd} A & B \arrow[l, "f"'] & C \arrow[l, "g"'] \arrow[ll, bend left, "f \circ g"] \end{tikzcd} \qquad \textit{dual :} \qquad \begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g \circ^{op} f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

in that

$$\begin{aligned} g \circ^{op} f \;\; of \;\; f &\in Hom_{\mathbf{A}^{op}}(A, B) \\ g &\in Hom_{\mathbf{A}^{op}}(B, C) \\ &then \\ g \circ^{op} f &= f \circ g \end{aligned}$$

e.g. if $\mathbf{A} = (M, \cdot, e)$ monoid, then $\mathbf{A}^{\text{op}} = (M, \hat{\cdot}, e)$ where $a \hat{\cdot} b = b \cdot a$

10.2.1. *Example.*

- Vec^{op}

$$\mathbf{Vec}^{\text{op}} = (\text{Obj}(\mathbf{Vec}), \text{Hom}_{\mathbf{Vec}^{\text{op}}}, 1, \circ^{\text{op}})$$

s.t.

$$\text{Hom}_{\mathbf{Vec}^{\text{op}}}(W, V) = \text{Hom}_{\mathbf{Vec}}(V, W)$$

$$\begin{tikzcd} U \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & V \arrow[r, "g"] & W \end{tikzcd} \qquad \begin{tikzcd} U & V \arrow[l, "f"'] & W \arrow[l, "g"'] \arrow[ll, bend left, "f \circ^{\text{op}} g"] \end{tikzcd}$$

10.3. **Kinds of morphisms.**

Definition 41 (isomorphism)**.** ***isomorphism*** *- morphism $f : A \to B$ is an isomorphism if $\exists g : B \to A$ s.t. $f \circ g = 1_B$, $g \circ f = 1_A$, g unique. g called inverse of f, f^{-1}*

$$1_A \circlearrowright \begin{tikzcd} A \arrow[r, "f"] & B \arrow[l, bend left, "g"] \end{tikzcd} \qquad 1_B \circlearrowright \begin{tikzcd} B \arrow[r, "g"] & A \arrow[l, bend left, "f"] \end{tikzcd}$$

Definition 42 (endomorphism)**.** ***endomorphism*** *- morphism with same source and target, that is, morphism $f : A \to A$*

Definition 43 (automorphism)**.** ***automorphism*** *- endomorphism which is an isomorphism*

Definition 44 (parallel)**.** ***parallel*** *- 2 morphisms f, g are parallel if they have same source and same target:*

$$\begin{aligned} f &: A \to B \\ g &: A \to B \end{aligned}$$

Definition 45 (monomorphism)**.** *monomorphism - morphism $f : A \to B$ is a monomorphism if $\forall$ pair of parallel $g_1 : C \to A$, $g_2 : C \to A$*

(40) $$f \circ g_1 = f \circ g_2 \textit{ implies } g_1 = g_2$$

i.e.

$$\begin{tikzcd} C \arrow[r, "f \circ g_1"] & B \arrow[l, bend left, "f \circ g_2"] \end{tikzcd} \quad \textit{implies } C \xrightarrow{g_1 = g_2} A$$

Definition 46 (epimorphism). ***epimorphism*** *- morphism $f : A \to B$ is an epimorphism if $f^{op} : B^{op} \to A^{op}$ is a monomorphism in $\mathbf{A}^{op}$.*

Hence f epimorphism iff $\forall$ parallel morphisms $\begin{aligned} g_1 &: B \to C \\ g_2 &: B \to C \end{aligned}$, $g_1 \circ f = g_2 \circ f$
implies $g_1 = g_2$

Proposition 15 (monomorphism, epimorphism iff injective). *f monomorphism iff $f\circ : Hom_{\mathbf{A}}(C, A) \to Hom_{\mathbf{A}}(C, B)$ injective $\forall C \in Obj(\mathbf{A})$, i.e.*

$$\begin{aligned} Hom_{\mathbf{A}}(C, A) &\xrightarrow{f\circ} Hom_{\mathbf{A}}(C, B) \\ g_1 = g_2 &\xmapsto{f\circ} f \circ g_1 = f \circ g_2 \end{aligned} \tag{41}$$

f epimorphism iff map $\circ f : Hom_{\mathbf{A}}(B, C) \to Hom_{\mathbf{A}}(A, C)$ injective $\forall C \in Obj(\mathbf{A})$

$$\begin{aligned} Hom_{\mathbf{A}}(B, C) &\xrightarrow{\circ f} Hom_{\mathbf{A}}(A, C) \\ g_1 = g_2 &\xmapsto{\circ f} g_1 \circ f = g_2 \circ f \end{aligned} \tag{42}$$

Definition 47 (inverses). *$\forall$ 2 morphisms, $f : X \to Y$, $g : Y \to X$ s.t. $f \circ g = 1_Y$,*
f is called left inverse of g, g is called right inverse of f.

We also say, g is a section of f, or f is a cosection of g.
f is an epimorphism, g is a monomorphism.

10.4. More definitions with categories.

Definition 48 (subcategory). *category $\mathbf{A}'$, $\mathbf{A}' \subset \mathbf{A}$, if $Obj(\mathbf{A}') \subset Obj(\mathbf{A})$, $Hom_{\mathbf{A}'}(A, B) \subset Hom_{\mathbf{A}}(A, B)$, $\forall A, B \in \mathbf{A}'$.*

Composition in $\mathbf{A}'$ is induced by composition in $\mathbf{A}$.
identity morphisms in $\mathbf{A}'$ are identity morphisms in $\mathbf{A}$

Definition 49 (full subcategory). *subcategory $\mathbf{A}'$ of $\mathbf{A}$ is full if $Hom_{\mathbf{A}'}(A, B) = Hom_{\mathbf{A}}(A, B)$, $\forall A, B \in \mathbf{A}'$*

Definition 50 (saturated subcategory). *full subcategory $\mathbf{A}'$ of $\mathbf{A}$ saturated if $A \in \mathbf{A}$ belongs to $\mathbf{A}'$ whenever A is isomorphic to object of $\mathbf{A}'$*

Definition 51 (discrete category). ***discrete*** *- discrete category if all morphisms are identity morphisms.*

Definition 52 (nonempty category). ***nonempty*** *- nonempty category if $Obj(\mathbf{A})$ is nonempty*

Definition 53 (groupoid). ***groupoid*** *- category $\mathbf{A}$ is a* ***groupoid*** *if all morphisms are isomorphisms.*

Definition 54 (finite category). *finite - finite category if set of all morphisms in $\mathbf{A}$ (hence, in particular, set of objects) is a finite set*

Definition 55 (connected). *connected category $\mathbf{A}$ if it's nonempty, and $\forall A, B \in Obj\mathbf{A}$, $\exists$ finite sequence of objects $(A_0 \dots A_n)$, $A_0 = A$, $A_n = B$, s.t. at least 1 of the sets $Hom_{\mathbf{A}}(A_j, A_{j+1})$ or $Hom_{\mathbf{A}}(A_{j+1}, A_j)$ is nonempty $\forall j \in \mathbb{N}$, with $0 \leq j \leq n-1$*

Definition 56 (monoid M). ***monoid*** *M (set endowed with internal product with associative and unital law) is nothing but a category with only 1 object (to M, associate category $\mathbf{M}$, with single object A, and morphisms $Hom_{\mathbf{M}}(A, A) = M$)*

Part 3. Reading notes on Cox, Little, O'Shea's *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*

11. Geometry, Algebra, and Algorithms

11.1. Polynomials and Affine Space.

fields are important is that linear algebra works over *any* field

Definition 57 (2). *set of all polynomials in $x_1, \dots, x_n$ with coefficients in k, denoted $k[x_1, \dots, x_n]$*

polynomial f *divides* polynomial g provided $g = fh$ for some $h \in k[x_1, \dots, x_n]$
$k[x_1, \dots, x_n]$ satisfies all field axioms except for existence of multiplicative inverses; commutative ring, $k[x_1, \dots, x_n]$ *polynomial ring*

Exercises for 1. **Exercise 1.** $\mathbb{F}_2$ commutative ring since it's an abelian group under addition, commutative in multiplication, and multiplicative identity exists, namely 1. It is a field since for $1 \neq 0$, the multiplicative identity is 1.

Exercise 2.

(a)
(b)
(c)

11.2. Affine Varieties.

11.3. Parametrizations of Affine Varieties.

11.4. Ideals.

11.5. Polynomials of One Variable.

12. Groebner Bases

12.1. Introduction.

12.2. Orderings on the Monomials in $k[x_1, \dots, x_n]$.

12.3. A Division Algorithm in $k[x_1, \dots, x_n]$.

12.4. Monomial Ideals and Dickson's Lemma.

12.5. The Hilbert Basis Theorem and Groebner Bases.

12.6. Properties of Groebner Bases.

12.7. Buchberger's Algorithm.

13. Elimination Theory

13.1. The Elimination and Extension Theorems.

13.2. The Geometry of Elimination.

14. The Algebra-Geometry Dictionary

14.1. Hilbert's Nullstellensatz.

14.2. Radical Ideals and the Ideal-Variety Correspondence.

15. Polynomial and Rational Functions on a Variety

15.1. Polynomial Mappings.

16. Robotics and Automatic Geometric Theorem Proving

16.1. Geometric Description of Robots.

Part 4. Reading notes on Cox, Little, O'Shea's *Using Algebraic Geometry*

Using Algebraic Geometry. David A. Cox. John Little. Donal O'Shea. Second Edition. Springer. 2005. ISBN 0-387-20706-6 QA564.C6883 2004

17. Introduction

17.1. Polynomials and Ideals. *monomial*

$$x_1^{\alpha_1} \dots x_n^{\alpha_n} \quad (1.1) \tag{43}$$

total degree of x^α is $\alpha_1 + \dots + \alpha_n \equiv |\alpha|$

field k, $k[x_1 \dots x_n]$ collection of all polynomials in $x_1 \dots x_n$ with coefficients k.

polynomials in $k[x_1 \dots x_n]$ can be added and multiplied as usual, so $k[x_1 \dots x_n]$ has structure of commutative ring (with identity)
however, only nonzero constant polynomials have multiplicative inverses in $k[x_1 \dots x_n]$, so $k[x_1 \dots x_n]$ not a field
however set of rational functions $\{f/g | f, g \in k[x_1 \dots x_n], g \neq 0\}$ is a field, denoted $k(x_1 \dots x_n)$

so

$$f = \sum_\alpha c_\alpha x^\alpha$$

where $c_\alpha \in k$
so

$$f \in k[x_1 \dots x_n] = \{f | f = \sum_\alpha c_\alpha x^\alpha, x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}, c_\alpha \in k\}$$

f homogeneous if all monomials have same total degrees
polynomial f is homogeneous if all monomials have the *same total degree*

Given a collection of polynomials $f_1 \dots f_s \in k[x_1 \dots x_n]$, we can consider all polynomials which can be built up from these by multiplication by arbitrary polynomials and by taking sums

Definition 58 (1.3)**.** *Let* $f_1 \dots f_s \in k[x_1 \dots x_n]$
Let $\langle f_1 \dots f_s \rangle = \{p_1 f_1 + \dots + p_s f_s | p_i \in k[x_1 \dots x_n]$ *for* $i = 1 \dots s\}$

Exercise 1.

(a) $x^2 = x \cdot (x - y^2) + y \cdot (xy)$
(b)

$$p \cdot (x - y^2) = px - py^2$$

and for $pxy = (py)x$
(c)

$$p(y)(x - y^2) = p(y)x - p(y)y^2 \notin \langle x^2, xy \rangle$$

Exercise 2.

$$\sum_{i=1}^s p_i f_i + \sum_{j=1}^s q_j f_j = \sum_{i=1}^s (p_i + q_i) f_i, \quad p_i + q_i \in k[x_1 \dots x_n]$$

$\langle f_1 \dots f_s \rangle$ closed under sums in $k[x_1 \dots x_n]$

If $f \in \langle f_1 \dots f_s \rangle$,
$p \in k[x_1 \dots x_n]$

$$p \cdot f = p \sum_{i=1}^s q_j f_j = \sum_{i=1}^s p q_j f_j, \quad pq_j \in k[x_1 \dots x_n] \text{ so}$$
$$p \cdot f \in \langle f_1 \dots f_s \rangle$$

Done.

The 2 properties in Ex. 2 are defining properties of ideals in the ring $k[x_1 \dots x_n]$

Definition 59 (1.5)**.** *Let* $I \subset k[x_1 \dots x_n], \quad I \neq \emptyset$
I ideal if

(a) $f + g \in I, \quad \forall f, g \in I$
(b) $pf \in I, \quad \forall f \in I$, *arbitrary* $p \in k[x_1 \dots x_n]$

Thus $\langle f_1 \dots f_s \rangle$ is an ideal by Ex. 2.

we call it the ideal generated by $f_1 \dots f_s$.

Exercise 3. Suppose $\exists$ ideal J, $f_1 \dots f_s \in J$ s.t. $J \subset \langle f_1 \dots f_s \rangle$
if $f \in \langle f_1 \dots f_s \rangle$, $f = \sum_{i=1}^s p_i f_i, \quad p_i \in k[x_1 \dots x_n]$

$\forall i = 1 \dots s$, $p_i f_i \in J$ and so $\sum_{i=1}^s p_i f_i \in J$, by def. of J as an ideal.

$$\langle f_1 \dots f_s \rangle \subseteq J \qquad \Longrightarrow J = \langle f_1 \dots f_s \rangle$$

$\Longrightarrow \langle f_1 \dots f_s \rangle$ is smallest ideal in $k[x_1 \dots x_n]$ containing $f_1 \dots f_s$

Exercise 4. For $I = \langle f_1 \dots f_s \rangle$
$J = \langle g_1 \dots g_t \rangle$

$I = J$ iff $s = t$ and $\forall f \in I$, $f = \sum_{i=1}^t q_i g_i$ and if $0 = \sum_{i=1}^t q_i g_i$, $q_i = 0$, $\forall i = 1 \dots t$, and if $0 = \sum_{i=1}^s p_i f_i$, $p_i = 0$, $\forall i = 1 \dots s$

Definition 60 (1.6)**.**

$$\sqrt{I} = \{g \in k[x_1 \dots x_n] | g^m \in I \textit{ for some } m \geq 1\}$$

e.g. $x + y \in \sqrt{\langle x^2 + 3xy, 3xy + y^2 \rangle}$
in $\mathbb{Q}[x, y]$ since

$$(x+y)^3 = x(x^2 + 3xy) + y(3xy + y^2) \in \langle x^2 + 3xy, 3xy + y^2 \rangle$$

- (Radical Ideal Property) $\forall$ ideal $I \subset k[x_1 \dots x_n]$, $\sqrt{I}$ ideal, $\sqrt{I} \supset I$
- **(Hilbert basis Thm.)** $\forall$ ideal $I \subset k[x_1 \dots x_n]$
  $\exists$ finite generating set,
  i.e. $\exists \{f_1 \dots f_2\} \subset k[x_1 \dots x_n]$ s.t. $I = \langle f_1 \dots f_s \rangle$

- (Division Algorithm in $k[x]$) $\forall f, g \in k[x]$ (EY : in 1 variable)
  $\forall f, g \in k[x]$ (in 1 variable)
  $f = qg + r$, $\exists!$ quotient q, $\exists$ remainder r

17.2.

17.3. Gröbner Bases.

Definition 61 (3.1). *Gröbner basis for $I \equiv G = \{g_1 \dots g_k\} \subset I$ s.t. $\forall f \in I$, $LT(f)$ divisible by $LT(g_i)$ for some i*

- (Uniqueness of Remainders) let ideal $I \subset k[x_1 \dots x_n]$
  division of $f \in k[x_1 \dots x_n]$ by Grö bner basis for I, produces $f = g + r$, $g \in I$, and no term in r divisible by any element of $\mathrm{LT}(I)$

17.4. **Affine Varieties.** affine n-dim. space over k $\quad k^n = \{(a_1 \dots a_n) | a_1 \dots a_n \in k\}$
$\forall$ polynomial $f \in k[x_1 \dots x_n]$, $(a_1 \dots a_n) \in k^n$
$f : k^n \to k$
$f(a_1 \dots a_n)$ s.t. $x_i = a_i$ i.e.

if $f = \sum_\alpha c_\alpha x^\alpha$ for $c_\alpha \in k$, then
$f(a_1 \dots a_n) = \sum_\alpha c_\alpha a^\alpha \in k$, where $a^\alpha = a_1^{\alpha_1} \dots a_n^{\alpha_n}$

Definition 62 (4.1). *affine variety $\mathbf{V}(f_1 \dots f_s) = \{(a_1 \dots a_n) | (a_1 \dots a_n) \in k^n, f_1(x_1 \dots x_n) = \dots = f_s(x_1 \dots x_n) = 0\}$ subset $V \subset k^n$ is affine variety if $V = V(f_1 \dots f_s)$ for some $\{f_i\}$, polynomial $f_i \in k[x_1 \dots x_n]$*

- (Equal Ideals Have Equal Varieties) If $\langle f_1 \dots f_s \rangle = \langle g_1 \dots g_t \rangle$ in $k[x_1 \dots x_n]$, then $\mathbf{V}(f_1 \dots f_s) = \mathbf{V}(g_1 \dots g_t)$

so, recap
if $\langle f_1 \dots f_s \rangle = \langle g_1 \dots g_t \rangle$ in $k[x_1 \dots x_n]$,
then $V(f_1 \dots f_s) = V(g_1 \dots g_t)$

Recall Hilbert basis Thm. $\forall$ ideal $I \subset k[x_1 \dots x_n]$

$$I = \langle f_1 \dots f_s \rangle$$

$\Longrightarrow$ if $I = J$, then $V(I) = V(J)$
think of V defined by I, rather than $f_1 = \dots = f_s = 0$

Exercise 3.
Recall Def. 1.5 Let $I \subset k[x_1 \dots x_n]$

I ideal if $f + g \in I \quad \forall f, g \in I$
$pf \in I, \quad \forall f \in I$ arbitrary $p \in k[x_1 \dots x_n]$
Let $f, g \in I(V)$

$$(f+g)(a_1 \dots a_n) = f(a_1 \dots a_n) + g(a_1 \dots a_n) = 0 + 0 = 0 \qquad f + g \in I(V)$$
$$pf(a_1 \dots a_n) = p(a_1 \dots a_n) f(a_1 \dots a_n) = 0 \qquad pf \in I(V)$$

Then $I(V)$ an ideal.
$V = V(x^2)$ in $\mathbb{R}^2$
$I = \langle x^2 \rangle$ in $\mathbb{R}[x, y]$, $\quad I = \{px^2 | p \in k[x, y]\}$
$I \subset I(V)$, since $px^2 = 0$ for $x^2 = 0$, $(0, b)$, $\quad b \in \mathbb{R}$
But $p(x, y) = x \in I(V)$, as

$$I(V) = \{f \in k[x_1 \dots x_n] | f(a_1 \dots a_n) = 0, \forall (a_1 \dots a_n) \in V\}$$

$p(0, b) = x = 0$
But $x \notin I$

Exercise 4. $I \subset \sqrt{I}$

Recall Def. 1.6 $\sqrt{I} = \{g \in k[x_1 \dots x_n] | g^m \in I \text{ for some } m \geq 1\}$
$\forall f \in I$, $f = f^1$, $m = 1$, so $f \in \sqrt{I}$, $\qquad I \subset \sqrt{I}$
Hilbert basis thm., $\forall$ ideal $I \subset k[x_1 \dots x_n]$ s.t. $I = \langle f_1 \dots f_s \rangle$
$\left\{ {}^{V(I) = \{(a_1 \dots a_n) | (a_1 \dots a_n) \in k^n, f_1(a_1 \dots a_n) = \dots = f_s(a_1 \dots a_n) = 0} \right\}$
$\mathbf{I}(\mathbf{V}(I)) = \{f \in k[x_1 \dots x_n] | f(a_1 \dots a_n) = 0 \quad \forall (a_1 \dots a_n) \in V(I)\}$
Let $g \in \sqrt{I}$, $\quad g^m \in I$, $\quad g^m = g^{m-1} g$
$g^m(a_1 \dots a_n) = 0 = g^{m-1}(a_1 \dots a_n) g(a_1 \dots a_n) = 0$. Then $g(a_1 \dots a_n) = 0$ or $g^{m-1}(a_1 \dots a_m) = 0$
as $g^m \in I$, and $V(I)$ is s.t. $f_1(a_1 \dots a_n) = \dots = f_s(a_1 \dots a_n) = 0$ for $I = \langle f_1 \dots f_s \rangle$

- (Strong Nullstellensatz) if k algebraically closed (e.g. $\mathbb{C}$), I ideal in $k[x_1 \dots x_n]$, then

$$\mathbf{I}(\mathbf{V}(I) = \sqrt{I}$$

- (Ideal-variety correspondence) Let k arbitrary field

$$I \subset I(V(I))$$
$$V(I(V)) = V \quad \forall V$$

Additional Exercises for Sec.4. Exercise 6.

18. Solving Polynomial Equations

18.1.

18.2. **Finite-Dimensional Algebras.** Gröbner basis $G = \{g_1 \dots g_t\}$ of ideal $I \subset k[x_1 \dots x_n]$,
recall def.: Gröbner basis $G = \{g_1 \dots g_t\} \subset I$ of ideal I, $\quad \forall f \in I$, $\mathrm{LT}(f)$ divisible by $\mathrm{LT}(g_i)$ for some i
$f \in k[x_1 \dots x_n]$ divide by G produces $f = g + r$, $g \in I$, r not divisible by any $\mathrm{LT}(I)$ uniqueness of r
$f \in k[x_1 \dots x_n]$ divide by G,
Recall from Ch. 1, divide $f \in k[x_1 \dots x_n]$ by G, the division algorithm yields

$$(44) \qquad (2.1) \qquad f = h_1 g_1 + \dots + h_t g_t + \overline{f}^G$$

where remainder $\overline{f}^G$ is a linear combination of monomials $x^\alpha \notin \langle \mathrm{LT}(I) \rangle$
since Gröbner basis, $f \in I$ iff $\overline{f}^G = 0$
$\forall f \in k[x_1 \dots x_n]$, we have coset $[f] = f + I = \{f + h | h \in I\}$ s.t. $[f] = [g]$ iff $f - g \in I$
We have a 1-to-1 correspondence

$$\text{remainders} \leftrightarrow \text{cosets}$$
$$\overline{f}^G \leftrightarrow [f]$$

algebraic

$$\overline{f}^G + \overline{g}^G \leftrightarrow [f] + [g]$$
$$\overline{\overline{f}^G \cdot \overline{g}^G} \leftrightarrow [f] \cdot [g]$$

$B = \{x^\alpha | x^\alpha \notin \langle \mathrm{LT}(I) \rangle\}$ is a basis of A, basis monomials, standard monomials
20141023 EY's take
$\forall [f] \in A = k[x_1 \dots x_n]/I$, $\quad [f] = p_i b_i$; $\quad b_i \in B = \{x^\alpha | x^\alpha \notin \langle \mathrm{LT}(I) \rangle\}$
For $I = \langle G \rangle$
e.g. $G = \{x^2 + \frac{3}{2}xy + \frac{1}{2}y^2 - \frac{3}{2}x - \frac{3}{2}y, xy^2 - x, y^3 - y\}$
$\langle \mathrm{LT}(I) \rangle = \langle x^2, xy^2, y^3 \rangle$
e.g. $B = \{1, x, y, xy, y^2\}$
$[f] \cdot [g] = [fg]$
e.g. $f = x$, $g = xy$, $[fg] = [x^2 y]$
now $f = h_1 g_1 + \dots + h_t g_t + \overline{f}^G$

18.3.

18.4. **Solving Equations via Eigenvalues and Eigenvectors.**

19. Resultants

20. Computation in Local Rings

20.1. **Local Rings.**

Definition 63 (1.1).

$$k[x_1 \dots x_n]_{\langle x_1 \dots x_n\rangle} \equiv \{ \frac{f}{g} | \textit{ rational functions } \frac{f}{g} \textit{ of } x_1 \dots x_n \textit{ with } g(p) \neq 0 \textit{ at } p \}$$

main properties of $k[x_1 \dots x_n]_{\langle x_1 \dots x_n \rangle}$

Proposition 16 (1.2). *Let $R = k[x_1 \dots x_n]_{\langle x_1 \dots x_n\rangle}$. Then*
(a) *R subring of field of rational functions $k(x_1 \dots x_n) \supset k[x_1 \dots x_n]$*
(b) *Let $M = \langle x_1 \dots x_n \rangle \subset R$ (ideal generated by $x_1 \dots X_n$ in R)*
Then $\forall \frac{f}{g} \in R \backslash M$, $\frac{f}{g}$ unit in R (i.e. multiplicative inverse in R)
(c) *M maximal ideal in R*

Exercise 1. if $p = (a_1 \dots a_n) \in k^n$, $R = \{ \frac{f}{g} | f, g \in k[x_1 \dots x_n], \, g(p) \neq 0 \}$
(a) R subring of field of rational functions $k(x_1 \dots x_n)$
(b) Let M ideal generated by $x_1 - a_1 \dots x_n - a_n$ in R
Then $\forall \frac{f}{g} \in R \backslash M$, $\frac{f}{g}$ unit in R (i.e. multiplicative inverse in R)
(c) M maximal ideal in R

Proof. let $p = (a_1 \dots a_n) \in k^n$
let $g_1(p) \neq 0$, $g_2(p) \neq 0$

$$\begin{aligned} \frac{f_1}{g_1} + \frac{f_2}{g_2} &= \frac{f_1 g_2 + f_2 g_1}{g_1 g_2} \qquad g_1(p)g_2(p) \neq 0 \text{ so } \frac{f_1}{g_1} + \frac{f_2}{g_2} \in R \\ \frac{f_1}{g_1} \cdot \frac{f_2}{g_2} &= \frac{f_1 f_2}{g_1 g_2} \qquad g_1(p)g_2(p) \neq 0 \text{ so } \frac{f_1}{g_1}\frac{f_2}{g_2} \in R \end{aligned}$$

$f = \frac{f}{I} \in R, \qquad \forall f \in k[x_1 \dots x_n]$, so $k[x_1 \dots x_n] \subset R$

EY : 20141027, to recap,
Let $V = k^n$
Let $p = (a_1 \dots a_n)$
single pt. $\{p\}$ is (an example of) a variety
$I(\{p\}) = \{x_1 - a_1 \dots x_n - a_n\rangle \subset k[x_1 \dots x_n]$

$R \equiv k[x_1 \dots x_n]_{\langle x_1 - a_1 \dots x_n - a_n \rangle}$

$$R = \{ \frac{f}{g} | \text{ rational function } \frac{f}{g} \text{ of } x_1 \dots x_n, \, g(p) \neq 0, \, p = (a_1 \dots a_n) \, \}$$

Prop. 1.2. properties
(a) R subring of field of rational functions $k(x_1 \dots x_n) \qquad k(x_1 \dots x_n) \subset R$
(b) $M = \langle x_1 \dots a_1 \dots x_n - a_n \rangle \subset R$. ideal generated by $x_1 - a_1 \dots x_n - a_n$
Then $\forall \frac{f}{g} \in R \backslash M$, $\frac{f}{g}$ unit in R ($\exists$ multiplicative inverse in R)
(c) M maximal ideal in R.
in R we allow denominators that are not elements of this ideal $I(\{p\})$

Definition 64 (1.3). *local ring is a ring that has exactly 1 maximal ideal*

Proposition 17 (1.4). *ring R with proper ideal $M \subset R$ is local ring if $\forall \frac{f}{g} \in R \backslash M$ is unit in R*

localization Ex. 8, Ex. 9
parametrization

Exercise 2.

$$\begin{aligned} x = x(t) &= \frac{-2t^2}{1+t^2} \\ y = y(t) &= \frac{2t}{1+t^2} \end{aligned}$$

$k[t]_{\langle t \rangle} \quad \frac{-2t^2}{1+t^2}$ rational function of t. $1 + t^2 \neq 0$
if $k = \mathbb{C}$ or $\mathbb{R}$

Consider set of convergent power series in n variables

$$(45) \qquad (1.5) \qquad k\{x_1 \dots x_n\} = \{ \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha | c_\alpha \in k, \text{ series converges in some open } U \ni 0 \in k^n \; \}$$

Consider set $k[[x_1 \dots x_n]]$ of formal power series

$$(46) \qquad (1.6) \qquad k[[x_1 \dots x_n]] = \{ \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha | c_\alpha \in k \} \text{ series need not converge}$$

variety V

$k[x_1 \dots x_n]/\mathbf{I}(V) \qquad$ variety V

□

20.2. **Multiplicities and Milnor Numbers.** if I ideal in $k[x_1 \dots x_n]$, then denote $Ik[x_1 \dots x_n]_{\langle x_1 \dots x_n \rangle}$ ideal generated by I in larger ring $k[x_1 \dots x_n]_{\langle x_1 \dots x_n \rangle}$

Definition 65 (2.1). *Let I 0-dim. ideal in $k[x_1 \dots x_n]$, so $V(I)$ consists of finitely many pts. in k^n.*
Assume $(0 \dots 0) \in V(I)$
multiplicity of $(0 \dots 0) \in V(I)$ is

$$dim_k k[x_1 \dots x_n]_{\langle x_1 \dots x_n \rangle} / I k[x_! \dots x_n]_{\langle x_1 \dots x_n \rangle}$$

generally, if $p = (a_1 \dots a_n) \in V(I)$
multiplicity of p, $m(p) = \dim k[x_1 \dots x_n]_M / I k[x_1 \dots x_n]_M$

$$\dim k[x_1 \dots x_n]_M / Ik[x_1 \dots x_n]_M$$

localizing $k[x_1 \dots x_n]$ at maximal ideal $M = I(\{p\}) = \langle x_1 - a_1 \dots x_n - a_n \rangle$

21.

22.

23. Polytopes, Resultants, and Equations

24. Polyhedral Regions and Polynomials

24.1. **Integer Programming.** Prop. 1.12.

Suppose 2 customers A, B ship to same location
A: ship 400 kg pallet taking up $2\,m^3$ volume
B: ship 500 kg pallet taking up $3\,m^3$ volume

shipping firm trucks carry up to 3700 kg, up to $20\,m^3$

B's product more perishable, paying \$ 15 per pallet

A pays \$ 11 per pallet
How many pallets from A, B each in truck to maximize revenues?

$$\begin{aligned} 4A + 5B &\leq 37 \\ 2A + 3B &\leq 20 \\ A, B &\in \mathbb{Z}^*_{\geq 0} \end{aligned} \quad (1.1) \qquad (47)$$

maximize $11A + 15B$

integer programming.
max. or min. value of some linear function

$$l(A_1 \dots A_n) = \sum_{i=1}^n c_i A_i$$

on set $(A_1 \dots A_n) \in \mathbb{Z}^n_{\geq 0}$ s.t.

3. Finally, by introducing additional variables; rewrite linear constraint inequalities as equalities. The new variables are called "slack variables"

$$a_{ij} A_j = b_i, \quad A_j \in \mathbb{Z}_{\geq 0} \quad (1.4) \qquad (48)$$

introduce indeterminate z_i, $\forall$ equation in (1.4)

$$z_i^{a_{ij} A_j} = z_i^{b_i}$$

m constraints

$$\prod_{i=1}^m z_i^{a_{ij} A_j} = \prod_{i=1}^m z_i^{b_i} = \left(\prod_{i=1}^m z_i^{a_{ij}} \right)^{A_j}$$

Proposition 18 (1.6)**.** *Let k field, define $\varphi : k[w_1 \dots w_n] \to k[z_1 \dots z_m]$ by*

$$\varphi(w_j) = \prod_{i=1}^m z_i^{a_{ij}} \qquad \forall\, j = 1 \dots n$$

and

$$\varphi(g(w_1 \dots w_n)) = g(\varphi(w_1) \dots \varphi(w_n))$$

$\forall$ general polynomial $g \in k[w_1 \dots w_n]$

Then $(A_1 \dots A_n)$ integer pt. in feasible region iff $\varphi : w_1^{A_1} \dots w_n^{A_n} \mapsto z_1^{b_1} \dots z_m^{b_m}$

Exercise 3.
Now

$$\varphi(w_j) = \prod_{i=1}^m z_i^{a_{ij}}$$
$$z_i^{a_{ij} A_j} = z_i^{b_i}$$

If $(A_1 \dots A_n)$ an integer pt. in feasible region, $a_{ij} A_j = b_i$

$$z_i^{a_{ij} A_j} = z_i^{b_i} = \prod_{j=1}^n z_i^{a_{ij} A_j} \Longrightarrow \prod_{j=1}^n \prod_{i=1}^m (z_i^{a_{ij}})^{A_j} = \prod_{i=1}^m z_i^{b_i} = \prod_{j=1}^n \varphi(w_j)^{A_j} = \prod_{j=1}^n \varphi(w_j)^{A_j} = \varphi \left(\prod_{j=1}^n w_j^{A_j} \right) = \prod_{i=1}^m z_i^{b_i}$$

since $\varphi(g(w_1 \dots w_n)) = g(\varphi(w_1) \dots \varphi(w_n))$

If $\varphi : \prod_{j=1}^n w_j^{A_j} \mapsto \prod_{i=1}^m z_i^{b_i}$

$$\varphi \left(\prod_{j=1}^n w_j^{A_j} \right) = \prod_{j=1}^n (\varphi(w_j))^{A_j} = \prod_{i=1}^m z_i^{b_i} = \prod_{j=1}^n \left(\prod_{i=1}^m z_i^{a_{ij}} \right)^{A_j} \Longrightarrow \prod_{j=1}^n z_i^{a_{ij} A_j} = z_i^{b_i}$$

or $a_{ij} A_j = b_i$. So $(A_1 \dots A_n)$ integer pt.

Exercise 4.

$$\prod_{i=1}^m z_i^{b_i} = \prod_{i=1}^m \prod_{j=1}^n z_i^{a_{ij} A_j} = \prod_{j=1}^n \left(\prod_{i=1}^m z_i^{a_{ij}} \right)^{A_j} = \prod_{j=1}^n \varphi(w_j)^{A_j} = \varphi \left(\prod_{j=1}^n w_j^{A_j} \right)$$

So if given $(b_1 \dots b_m) \in \mathbb{Z}^m$, and for a given a_{ij}, $a_{ij} A_j = b_i$

For $m \leq n$, then a_{ij} is surjective, so $\exists\, A_j$ s.t. $\prod_{i=1}^m z_i^{b_i} = \varphi \left(\prod_{j=1}^n w_j^{A_j} \right)$

Proposition 19 (1.8)**.** *Suppose $f_1 \dots f_n \in k[z_1 \dots z_m]$ given*
Fix monomial order in $k[z_1 \dots z_n, w_1 \dots w_n]$ with elimination property:
$\forall$ monomial containing 1 of z_i greater than any monomial containing only w_j

Let $\mathcal{G}$ Gröbner basis for ideal

$$I = \langle f_1 - w_1 \dots f_n - w_n \rangle \subset k[z_1 \dots z_m, w_1 \dots w_n]$$

$\forall\, f \in k[z_1 \dots z_m]$, let $\overline{f}^{\mathcal{G}}$ be remainder on division of f by $\mathcal{G}$
Then

(a) *polynomial f s.t. $f \in k[f_1 \dots f_n]$ iff $g = \overline{f}^{\mathcal{G}} \in k[w_1 \dots w_n]$*

(b) *if $f \in k[f_1 \dots f_n]$ as in part (a),*
$g = \overline{f}^{\mathcal{G}} \in k[w_1 \dots w_n]$
then $f = g(f_1 \dots f_n)$, giving an expression for f as polynomial in f_j

(c) *if $\forall\, f_i, f$ monomials, $f \in k[f_1 \dots f_n]$,*
then g also a monomial.

24.2. Integer Programming and Combinatorics.

25. Algebraic Coding Theory

26. The Berlekamp-Massey-Sakata Decoding Algorithm

Gröbner Bases, Martin R. Albrecht of the DTU Crypto Group

Part 5. Statistical Mechanics: Ising Model

27. Ising Model

27.1. Definition of Ising Model.

cf. Wikipedia, "Ising model"

Consider set of lattice sites Λ, each with set of adjacent sites (e.g. **graph**) forming d-dim. lattice.
$\forall$ lattice site $k \in \Lambda$, $\exists$ discrete variable σ_k, s.t. $\sigma_k \in \{-1,1\}$.
spin configuration $\equiv \sigma = (\sigma_k)_{k\in\Lambda}$ is an assignment of spin value to each lattice site.

i.e.

$d=1$, consider "line" configuration: $i \in \mathbb{Z}$, $i = 0,1,\dots L-1$. Lattice site $k \in \Lambda = \Lambda_{d=1}$. $\forall k \in \Lambda$, $\exists$ bijection to its index i, $k \mapsto i$, and $\exists \sigma_k$ i.e.

$$\begin{aligned} \sigma : \Lambda \leftrightarrow \sigma : \mathbb{Z} \to \mathbb{Z}_2 \\ \sigma(k) \equiv \sigma_k \leftrightarrow \sigma(i) \equiv \sigma_i \mapsto \{-1,1\} \end{aligned}$$

spin configuration $\sigma : \Lambda \mapsto (\sigma_k)_{k\in\Lambda} \in \{-1,1\}^{|\Lambda|}$, where $|\Lambda| = L$.
$\forall k \in \Lambda$, $\exists !$ only at most 2 edges, given, for $k \mapsto i$, $i+1, i-1$, $\forall i = 1\dots L-2$.

$d=2$, "rectangle" configuration. $(i,j) \in \mathbb{Z}^2$. $\begin{aligned} i \in 0,1,\dots L_x - 1 \\ j \in 0,1,\dots L_y - 1 \end{aligned}$. Lattice site $\mathbf{k} \in \Lambda = \Lambda_{d=2}$.
$\forall \mathbf{k} \in \Lambda$, $\exists$ bijection to its "grid coordinates" (i,j), $\mathbf{k} \mapsto (i,j)$, and $\exists \sigma_{\mathbf{k}}$ i.e. $\sigma_{\mathbf{k}} = \sigma_{ij} \in \{-1,1\}$.
spin configuration $\sigma : \Lambda \mapsto (\sigma_{\mathbf{k}})_{\mathbf{k}\in\Lambda} \in \{-1,1\}^{|\Lambda|}$, where $|\Lambda| \equiv |\Lambda_{d=2}| = L_x L_y$.

$\forall \mathbf{k} \in \Lambda$, $\exists !$ only at most 4 edges, given by $\mathbf{k} \mapsto (i,j)$, $(i\pm 1, j), (i, j\pm 1)$, $\begin{aligned} i = 1\dots L_x - 2 \\ j = 1 \dots L_y - 2 \end{aligned}$.

Note that in both cases, I haven't yet defined the boundary conditions, and leave that to be discussed thoroughly in the future (i.e. following sections).

There are $2^{|\Lambda|}$ number of configurations in any dim. d.

cf. Wikipedia, "Ising model"

27.1.1. *Interaction $J_{ij} \equiv J_{\mathbf{kl}}$, Hamiltonian (energy functional)for a configuration $H(\sigma)$.*

$\forall$ 2 adjacent (lattice) sites, $i, j \equiv \mathbf{k}, \mathbf{l} \in \Lambda$, let there be an interaction $J_{ij} \equiv J_{\mathbf{kl}}$ i.e. $\begin{aligned} J : \Lambda^2 \to \mathbb{R} \\ J : (\mathbf{k},\mathbf{l}) \mapsto J_{\mathbf{kl}} \end{aligned}$.
Adjacent means $\exists$ edge $\mathbf{k} \mapsto \mathbf{l}$ (the mapping is the edge)

Suppose $\forall$ site $j \equiv \mathbf{l} \in \Lambda$, $\exists$ external magnetic field $h_j \equiv h_{\mathbf{l}}$ interacting with it.
Given (site) configuration $\sigma : \Lambda \mapsto (\sigma_{\mathbf{k}})_{\mathbf{k}\in\Lambda} \in \{-1,1\}^{|\Lambda|}$.

$$H(\sigma) = -\sum_{\langle ij\rangle} J_{ij}\sigma_i\sigma_j - \mu \sum_j h_j \sigma_j \equiv H(\sigma(\Lambda)) = -\sum_{\langle \mathbf{kl}\rangle} J_{\mathbf{kl}}\sigma_{\mathbf{k}}\sigma_{\mathbf{l}} - \mu \sum_{\mathbf{k}\in\Lambda} h_{\mathbf{k}}\sigma_{\mathbf{k}} \tag{49}$$

where $\sum_{\langle \mathbf{kl}\rangle}$ is overall pairs of adjacent spins (every pair is counted once),
$\langle \mathbf{k},\mathbf{l}\rangle \equiv$ sites $\mathbf{k},\mathbf{l}$ are nearest neighbors.

Note sign in 2nd. term, $-\mu\sum_{\mathbf{k}} h_{\mathbf{k}}\sigma_{\mathbf{k}}$ should be positive because of electron's magnetic moment is antiparallel to its spin, but negative term used conventionally.

Nothing was said about boundary conditions, I propose that it can be either fixed in the summation or by setting $J_{\mathbf{kl}} = 0$.

$\forall \mathbf{k} \in \Lambda$, let $\begin{aligned} \mathbf{y} : \Lambda \to E \\ \mathbf{y} : \mathbf{k} \mapsto \{\langle \mathbf{k},\mathbf{l}\rangle\}_{\mathbf{l}} \end{aligned}$, with $\{\langle \mathbf{k},\mathbf{l}\rangle\}_{\mathbf{l}}$ be set of all edges from $\mathbf{k}$

Then clearly $\sum_{\langle \mathbf{kl}\rangle} = \frac{1}{2}\sum_{\mathbf{k}\in\Lambda}\sum_{\{\langle \mathbf{kl}\rangle\}_{\mathbf{l}}}$.
Taking into account only interaction between adjoining dipoles, on a square lattice:

$$E(\sigma) = -J\sum_{k,l=0}^{L-1}(\sigma_{kl}\sigma_{k,l+1} + \sigma_{kl}\sigma_{k+1,l})$$

cf. Landau and Lifshitz [9]

EY : 20171223 Things to check from Hjorth-Jensen (2015) [10]:

2-dim. Ising model, with $\mathcal{B} \equiv h_j = 0$, undergoes phase transition of 2nd. order: meaning below given critical temperature T_C, there's spontaneous magnetization with $\langle \mathcal{M}\rangle \equiv \langle \mathbf{M}\rangle \neq 0$. $\langle \mathbf{B}\rangle \to 0$ at T_C with *infinite* slope, a behavior called *critical phenomena*. Critical phenomenon normally marked by 1 or more thermodynamical variables which is 0 above a critical point. In this case, $\langle \mathbf{B}\rangle \neq 0$, such a parameter normally called *order parameter*.

Critical phenomena; we still don't have a satisfactory understanding of system's properties close to the critical point, even for simplest 3-dim. systems. Even mean-field models can predict wrong physics; mean-field theory results in a 2nd.-order phase transition for 1-dim. Ising model, wherea 1-dim. Ising model doesn't predict any spontaneous magnetization at any finite temperature T.

e.g. Consider 1-dim. N-spin system. Assume periodic boundary conditions. Consider state of all spins up, with total energy $-NJ$ and magnetization N. Flip half of spins (e.g. all spins of index $i > N/2$) so 1st half of spins point upwards and last half points downwards. Energy is $-NJ + 4J$, net magnetization 0. This is an example of a possible disordered state with net magnetization 0. Change in energy is too small to stabilize disordered state (to $-NJ$).

Definition 66 (configuration probability). ***configuration probability*** *$P_\beta(\sigma)$ given by Boltzmann distribution:*

$$P_\beta(\sigma) = \frac{\exp(-\beta H(\sigma))}{Z_\beta} = \text{ prob. of configuration } \sigma \equiv \sigma(\Lambda) \equiv (\sigma_{\mathbf{k}})_{\mathbf{k}\in\Lambda} \tag{50}$$

with the partition function as normalization constant Z_β:

$$Z_\beta = \sum_\sigma \exp -\beta H(\sigma) \tag{51}$$

cf. pp. 504 Sec. 151 Phase transitions of the second kind in a 2-dim. lattice, Landau and Lifshitz [9]

$$Z = 2^N(1-x^2)^{-N}\prod_{p,q=0}^{L-1}\left[(1+x^2)^2 - 2x(1-x^2)\left(\cos\frac{2\pi p}{L} + \cos\frac{2\pi q}{L}\right)\right]^{1/2} \tag{52}$$

cf. (151.11) of Landau and Lifshitz [9], where $x = \tanh\theta$, $\theta = J/T \equiv J/\tau = \beta J$.

$$\begin{aligned} \Phi \equiv F = -\tau \ln Z = \\ = -\tau N \ln 2 + \tau N \ln(1-x^2) - \frac{\tau}{2}\sum_{p,q=0}^{L}\ln\left[(1+x^2)^2 - 2x(1-x^2)\left(\cos\frac{2\pi p}{L} + \cos\frac{2\pi q}{L}\right)\right] \end{aligned} \tag{53}$$

Let $\begin{aligned} \omega_1 = \frac{2\pi p}{L} \text{ with } p \to 0 \text{ as } L \to \infty \\ \omega_2 = \frac{2\pi q}{L} \text{ with } q \to 0 \text{ as } L \to \infty \end{aligned}$ so $\begin{aligned} \frac{L d\omega_1}{2\pi} = dp \\ \frac{L d\omega_2}{2\pi} = dq \end{aligned}$ and using $L^2 = N$.

$$\Phi = -\tau N \ln 2 + \tau N \ln(1-x^2) - \frac{N\tau}{2(2\pi)^2}\int_0^{2\pi}\int_0^{2\pi} d\omega_1 d\omega_2 \ln\left[(1-x^2) - 2x(1-x^2)(\cos\omega_1 + \cos\omega_2)\right]$$

$F \equiv \Phi$ has singularity when $(1-x^2) - 2x(1-x^2)(\cos\omega_1+\cos\omega_2)$ in $\ln\left[(1-x^2)-2x(1-x^2)(\cos\omega_1+\cos\omega_2)\right]$.
$(1-x^2)-2x(1-x^2)(\cos\omega_1+\cos\omega_2)$ minimized when $\cos\omega_1 = \cos\omega_2 = 1$ (since $-1 < x < 1$)

$$\Longrightarrow (1+x^2)^2 - 4x(1-x^2) = 1 + 2x^2 + x^4 - 4x + 4x^3 = (x^2+2x-1)^2 = 0 \Longrightarrow x = \frac{-2\pm\sqrt{4-4(-1)}}{2} = -1+\sqrt{2}$$

$$x = \tanh\theta = \frac{e^\theta - e^{-\theta}}{e^\theta + e^{-\theta}} = \sqrt{2}-1 \text{ or } \quad \begin{aligned} e^\theta - e^{-\theta} &= \sqrt{2}e^\theta + \sqrt{2}e^{-\theta} - e^\theta - e^{-\theta} \text{ so} \\ (2-\sqrt{2})e^\theta &= \sqrt{2}e^{-\theta} \\ e^{2\theta} &= \frac{\sqrt{2}}{2-\sqrt{2}}\left(\frac{2+\sqrt{2}}{2+\sqrt{2}}\right) \text{ or} \\ 2\theta &= \ln(1+\sqrt{2}) \end{aligned}$$

$$\frac{J}{T_c} = \frac{1}{2}\ln(1+\sqrt{2}) \text{ or}$$

$$\boxed{\tau_c = \frac{2J}{\ln(1+\sqrt{2})}} \tag{54}$$

so that $\tau_C \equiv T_C$ is where phase transition occurs.

Let $t := \tau - \tau_c$. $\theta = \frac{J}{\tau} = \frac{J}{t+\tau_C}$

Expand about minimum

EY:20171230 do this explicitly

$$\int_0^{2\pi}\int_0^{2\pi} d\omega_1 d\omega_2 \ln\left[c_1 t^2 + c_2(\omega_1^2+\omega_2^2)\right]$$

$$F \equiv \Phi \simeq a + \frac{1}{2}b(\tau-\tau_c)^2\ln|\tau-\tau_c|$$

$$C = \frac{\partial^2 F}{\partial\tau} \simeq -b\tau_c \ln|\tau-\tau_c|$$

with C being heat capacity.

Order parameter $\langle M\rangle \equiv \eta = \text{constant}(\tau_c-\tau)^{1/8} = \begin{cases} 0 & \text{if } \tau > \tau_c \\ \text{constant } (\tau_c-\tau)^{1/8} & \text{if } \tau < \tau_c \end{cases}$

cf. pp. 505 Sec. 151 Phase transitions of the second kind in a 2-dim. lattice, Landau and Lifshitz [9], L.Onsager 1947.

27.2. **An actual calculation of a small number of spins with Ising model.** Sec. 3.7 "An actual calculation" on pp. 76 of Newman and Barkema (1999) [11] goes through a simple actual Monte Carlo calculation as a test case check so to compare this exact calculation/solution to the simulation, as a test of whether the simulation/program is correct. This is done in Sec. 1.3 of Newman and Barkema (1999) [11].

However, none of these promised simple calculations were shown explicitly in Newman and Barkema (1999) [11]. I will forego this simple case.

27.3. **Explicit calculation showing stencil operation on each spin on a periodic lattice grid.** Consider

$$\begin{aligned} H(\sigma) &= -\sum_{\langle \mathbf{kl}\rangle} J\sigma_{\mathbf{k}}\sigma_{\mathbf{l}} = -J\sum_{i=0}^{L_x-1}\sum_{j=0}^{L_y-1}\sigma_{ij}(\sigma_{i+1j}+\sigma_{ij+1}) = \\ &= \frac{-J}{2}\left(\sum_{i=0}^{L_x-1}\sum_{j=0}^{L_y-1}\sigma_{ij}(\sigma_{i+1j}+\sigma_{ij+1}) + \sum_{i=1}^{L_x}\sum_{j=0}^{L_y-1}\sigma_{i-1j}(\sigma_{ij}+\sigma_{i-1j+1})\right) = \\ &= \frac{-J}{2}\left(\sum_{i=0}^{L_x-1}\sum_{j=0}^{L_y-1}\sigma_{ij}(\sigma_{i+1j}+\sigma_{ij+1}) + \sum_{i=1}^{L_x}\sum_{j=0}^{L_y-1}\sigma_{i-1j}\sigma_{ij} + \sum_{i=0}^{L_x-1}\sum_{j=1}^{L_y}\sigma_{ij-1}\sigma_{ij}\right) \end{aligned}$$

Now for each of these terms,

$$\sum_{i=1}^{L_x}\sum_{j=0}^{L_y-1}\sigma_{i-1j}\sigma_{ij} = \sum_{i=1}^{L_x}\left(\sum_{j=1}^{L_y-1}\sigma_{i-1j}\sigma_{ij} + \sigma_{i-10}\sigma_{i0}\right) = \sum_{i=1}^{L_x-1}\left(\sum_{j=1}^{L_y-1}\sigma_{i-1j}\sigma_{ij}+\sigma_{i-10}\sigma_{i0}\right) + \left(\sum_{j=1}^{L_y-1}\sigma_{L_x-1j}\sigma_{L_xj}\right) + \sigma_{L_x-10}\sigma_{L_x0}$$

$$\sum_{i=0}^{L_x-1}\sum_{j=1}^{L_y}\sigma_{ij-1}\sigma_{ij} = \sum_{j=1}^{L_y-1}\left(\sum_{i=1}^{L_x-1}\sigma_{ij-1}\sigma_{ij} + \sigma_{0j-1}\sigma_{0j}\right) + \sum_{i=1}^{L_x-1}\sigma_{iL_y-1}\sigma_{iL_y} + \sigma_{0L_y-1}\sigma_{0L_y}$$

$$\begin{aligned} \sum_{i=0}^{L_x-1}\sum_{j=0}^{L_y-1}\sigma_{ij}(\sigma_{i+1j}+\sigma_{ij+1}) &= \sum_{i=0}^{L_x-1}\left(\sum_{j=1}^{L_y}\sigma_{ij}(\sigma_{i+1j}+\sigma_{ij+1}) + \sigma_{i0}(\sigma_{i+10}+\sigma_{i1})\right) = \\ \sum_{i=1}^{L_x-1}&\left(\sum_{j=1}^{L_y-1}\sigma_{ij}(\sigma_{i+1j}+\sigma_{ij+1}) + \sigma_{i0}(\sigma_{i+10}+\sigma_{i1})\right) + \sum_{j=1}^{L_y-1}\sigma_{0j}(\sigma_{1j}+\sigma_{0j+1}) + \sigma_{00}(\sigma_{10}+\sigma_{01}) \end{aligned}$$

Apply periodic boundary conditions. Adding up all the terms above, clearly we obtain 1 term which shows the stencil operation for spins on the "interior" of the grid:

$$\sum_{i=1}^{L_x-1}\sum_{j=1}^{L_y-1}\sigma_{ij}(\sigma_{i+1j}+\sigma_{ij+1}+\sigma_{i-1j}+\sigma_{ij-1})$$

and if we apply *periodic* boundary conditions, neatly, we'll see all the lattice sites at the boundary also will have this stencil operation:

$$\begin{aligned} \sum_{i=1}^{L_x-1}\sigma_{i0}(\sigma_{i+10}+\sigma_{i1}) + \sum_{j=1}^{L_y-1}\sigma_{0j}(\sigma_{1j}+\sigma_{0j+1}) + \sigma_{00}(\sigma_{10}+\sigma_{01}) + \left(\sum_{i=1}^{L_x-1}\sigma_{iL_y-1}\sigma_{i0}\right) + \sigma_{0L_y-1}\sigma_{00} + \sum_{j=1}^{L_y-1}\sigma_{0j-1}\sigma_{0j} + \\ + \sum_{j=1}^{L_y-1}\sigma_{L_x-1j}\sigma_{0j} + \sigma_{L_x-10}\sigma_{00} + \sum_{i=1}^{L_x-1}\sigma_{i-10}\sigma_{i0} \end{aligned}$$

Now, we can obtain the following for Hamiltonian, given spin configuration σ with a lattice grid obeying periodic conditions:

$$H(\sigma) = -\frac{J}{2}\sum_{i=0}^{L_x-1}\sum_{j=0}^{L_y-1}\sigma_{ij}(\sigma_{i+1j}+\sigma i - 1j + \sigma_{ij+1}+\sigma_{ij-1}) =$$

(55)
$$= \frac{-J}{2}\left[\sum_{i=0}^{L_x-1}\left(\sum_{\substack{j=0\\ j\neq j'}}^{L_y-1}\sigma_{ij}(\sigma_{i+1j}+\sigma_{i-1j}+\sigma_{ij+1}+\sigma_{ij-1}) + \sigma_{ij'}(\sigma_{i+1j'}+\sigma_{i-1j'}+\sigma_{ij'+1}+\sigma_{ij'-1})\right) + \right.$$
$$\left.\sum_{\substack{j=0\\ j\neq j'}}^{L_y-1}\sigma_{i'j}(\sigma_{i'+1j}+\sigma_{i'-1j}+\sigma_{i'j+1}+\sigma_{i'j-1}) + \sigma_{i'j'}(\sigma_{i'+1j'}+\sigma_{i'-1j'}+\sigma_{i'j'+1}+\sigma_{i'j'-1})\right]$$

Consider a psin flip of $\sigma_{i'j'}$. Contribution to ΔH at stencil operation on $\sigma_{i'j'}$, at $(i'j')\in\Lambda$, is

$$\frac{-J}{2}(-\sigma_{i'j'}-\sigma_{i'j'})(\sigma_{i'+1j'}+\sigma_{i'-1j'}+\sigma_{i'j'+1}+\sigma_{i'j'-1}) = J\sigma_{i'j'}(\sigma_{i'+1j'}+\sigma_{i'-1j'}+\sigma_{i'j'+1}+\sigma_{i'j'-1})$$

Consider $\sigma_{i'j'}\sigma_{i'+1j'}$. Clearly, term $\sigma_{i-1j'}\sigma_{ij'}$ with $i=i'+1$ only occurs once more in the summation. Thus, we can definitely conclude that for $\Delta H \equiv \Delta H(\Delta\sigma_{i'j'})$ due to a single spin-flip is

(56)
$$\Delta H(\Delta \sigma_{i'j'}) = 2J\sigma_{i'j'}(\sigma_{i'+1j'}+\sigma_{i'-1j'}+\sigma_{i'j'+1}+\sigma_{i'j'-1})$$

https://www.colorado.edu/physics/phys7240/phys7240_fa12/notes/Week3.pdf Victor Gurarie, Advanced Statistical Mechanics, Fall 2012 Exact solution by transfer matrices for 2-dim. Ising model.

Part 6. Conformal Field Theory; Virasoro Algebra

cf. Schottenloher (2008) [8]

28. Conformal Transformations

Definition 67 (Conformal transformation or conformal map)**.** *Let 2 semi-Riemannian manifolds(M,g), (M',g'), $\dim M = \dim M'$, let open $U\subset M$, open $V\subset M'$.*

conformal transformation *or* ***conformal map*** *is a smooth $\varphi: U\to V$ of maximal rank, if $\exists$ smooth $\Omega: U\to\mathbb{R}^+$ s.t.*

(57)
$$\varphi^* g' = \Omega^2 g$$

where $\varphi * g'(X,Y) := g'(T\varphi(X), T\varphi(Y))$ and $T\varphi: TU\to TV$ denote tangent map (derivative) of φ.

$\Omega\equiv$ conformal factor *of φ.*

Locally, $y^i = \varphi^i(x)$,

$$\frac{\partial\varphi^i}{\partial x^j} = \frac{\partial y^i}{\partial x^j}$$

Then

$$X = X^k\frac{\partial}{\partial x^k} = X^k \frac{\partial y^i}{\partial x^k}\frac{\partial}{\partial y^i} = X^k\frac{\partial\varphi^i}{\partial x^k}\frac{\partial}{\partial y^k}\in TM$$

and so

$$\varphi^*g'(X,Y) = g'(T\varphi(X),T\varphi(Y)) = (g')_{ij}X^k\frac{\partial y^i}{\partial x^k}Y^l\frac{\partial y^j}{\partial x^l} = (g')_{ij}X^k\frac{\partial \varphi^i}{\partial x^k}Y^l\frac{\partial y^j}{\partial x^l}$$
$$\Longrightarrow (\varphi^*g')_{kl} = (g')_{ij}\frac{\partial y^i}{\partial x^k}\frac{\partial y^j}{\partial x^l}$$
$$\Longrightarrow (\varphi^*g')_{kl} = (g')_{ij}\frac{\partial \varphi^i}{\partial x^k}\frac{\partial \varphi^j}{\partial x^l} = \Omega^2 g_{kl}$$

Definition 68. ***extension*** *of G by group A is (given by) an* exact sequence *of group homomorphisms.*

$$1\longrightarrow A\xrightarrow{i} E\xrightarrow{\pi} G\longrightarrow 1$$

cf. Def. 3.1 of Schottenloher (2008) [8].

Recall that an exact sequence, if
$$\begin{aligned} &\mathrm{im}(1\to A) = \ker(i) \\ &\mathrm{im}(i) = \ker(\pi) \\ &\mathrm{im}(\pi) = \ker(G\to 1)\end{aligned}$$

By Thm., $1\to A\xrightarrow{i} E$ exact so i injective.
$E\xrightarrow{\pi} G\to 1$ exact so π surjective.
Extension is called **central** if A abelian and image $\mathrm{im} i$ is in center of E, i.e. $a\in A, b\in E\Longrightarrow i(a)b = bi(a)$.

28.0.1. *Examples of extensions of G, and central extensions of G (which has a particular E).*

- e.g. central extension has form

$$1\longrightarrow A\xrightarrow{i} A\times G\xrightarrow{\mathrm{pr}_2} G\longrightarrow 1$$

where
$i: A\to A\times G$
$a\mapsto (a,1)$

$$i(a)(a',g) = (a,1)(a',g) = (aa',g) =$$
$$= (a'a, g\cdot 1) = (a',g)(a,1) = (a',g)i(a)$$

Notice that what the *exactness* property of an exact sequence does:

$$\mathrm{pr}_2 i(a) = \mathrm{pr}_2(a,1) = 1$$

- e.g. of a nontrivial central extension is exact sequence

(58)
$$1\longrightarrow \mathbb{Z}/k\mathbb{Z}\longrightarrow E\times U(1)\xrightarrow{\pi} U(1)\longrightarrow 1$$

with $\pi(z) = z^k \quad \forall\, k\in\mathbb{N}$, $k\geq 2$, since $E=U(1)$ and $\mathbb{Z}/k\mathbb{Z}$ are not isomorphic.

Also, homomorphism $\tau: U(1)\to E$ with $\pi\circ\tau = 1_{U(1)}$, doesn't exist, since there's no global kth root.

EY : 20170926 It's that in integer division of the argument in a complex number $z\in U(1)$, and exponent multiplication by k, you go from 1 to many and many to 1, depending upon the "branch" you're mapping to for complex numbers.

For $[n]\in\mathbb{Z}/k\mathbb{Z}$,

$$[n]\xmapsto{i}\exp\left(\frac{[n]}{k}2\pi i\right)$$

and so

$$\ker\pi = \{z|\pi(z) = 1\} \text{ so that } \ker\pi = \{z = \exp\left(\frac{i2\pi n}{k}\right)\}$$

- e.g. *Semidirect products.*
group G acting on another group H, by homomorphism

$$\tau: G\to\mathrm{Aut}(H)$$

Definition 69 (semi-direct product)**.** ***semidirect product*** *group $G\ltimes H$ is set $H\times G$, with multiplication*

$$(x,g)\cdot(x',g') := (x\tau(g)(x'), gg') \qquad \forall\,(x,g),(x',g')\in H\times G$$

(59)
$$1 \longrightarrow H \xrightarrow{i} G \ltimes H \xrightarrow{\pi} G \longrightarrow 1$$

with

(60)
$$\begin{gathered} i: H \to G \ltimes H \\ i(x) = (x,1) \end{gathered}$$

i group homomorphism, since

$$i(x_1x_2) = (x_1x_2, 1) = (x_1 \tau(1) x_2, 1) = (x_1, 1)\cdot(x_2,1) = i(x_1)i(x_2)$$

(61)
$$\begin{gathered} \pi : G \ltimes H \to G \\ \pi(x,g) = g \end{gathered}$$

cf. http://sierra.nmsu.edu/morandi/oldwebpages/math683fall2002/GroupExtensions.pdf

Observe that

$$\pi i(x) = \pi(x,1) = 1 \text{ so } \ker\pi = \mathrm{im} i$$

Definition 70 (Semi-direct product (2); with direct product)**.** ***direct product*** *$G = HK$ if H,K subgroups of group G, s.t.*

- *H and K are normal in G ($gkg^{-1} \in K \quad \forall g \in G, \forall k \in K$)*
- *$H \cap K = \{1\}$*
- *$HK = G$.*

semi-direct product*. Relax the 1st condition (of direct products) so H still normal in G, but K need not be.*

- *H normal in G ($ghg^{-1} \in H, \forall g, \forall h \in H$)*
- *$H \cap K = \{1\}$*
- *$HK = G$*

Connection between Def. 69 and Def. 70 for the *semidirect product*: Consider $\tau : G \to \mathrm{Aut}(H)$.

Consider $G \ltimes H$ - what is the identity $1_{G\ltimes H} \equiv (1_H, 1_G)$ of this group?

$$(x,g)\cdot(1_H,1_G) = (x\tau(g)1_H, g1_G) = (x\tau(g)1_H, g) \Longrightarrow 1_H = \tau(g^{-1})1,\, 1_G = 1$$

and so the inverse, $\forall (x,g) \in G \ltimes H$, $(x,g)^{-1} \equiv ((x^{-1}),(g^{-1}))$,

$$(x,g)(x,g)^{-1} = (x\tau(g)(x^{-1}), g(g^{-1})) = (x\tau(g)(x^{-1}),1) \text{ (if } (g^{-1}) = g^{-1})$$

Moving along,

$$\begin{gathered} x\tau(g)(x^{-1}) = \tau(g^{-1})1 \\ \Longrightarrow (x^{-1}) = \tau(g^{-1})x^{-1}\tau(g^{-1})1 \end{gathered}$$

Checking out the H being a normal subgroup of $G \ltimes H$ condition, i.e. $H \lhd G$,

$$\begin{aligned} &(x,g)(h,1)(\tau(g^{-1})x^{-1}\tau(g^{-1}),g^{-1}) = (x\tau(g)h, g)(\tau(g^{-1})x^{-1}\tau(g^{-1}),g^{-1}) = \\ &= (x\tau(g)h\tau(g)\tau(g^{-1})x^{-1}\tau(g^{-1}),1) = (x\tau(g)hx^{-1}\tau(g^{-1}),1) \end{aligned}$$

$\Longrightarrow H$ normal subgroup of $G \ltimes H \equiv H \lhd (G \ltimes H)$.

Notes on Semidirect products

- extension

(62)
$$1 \longrightarrow SL(n,\mathbb{R}) \xrightarrow{i} GL(n,\mathbb{R}) \xrightarrow{\det} \mathbb{R}^* \longrightarrow 1$$

with

$GL(n,\mathbb{R}) \equiv Gl_n(\mathbb{R}) = \{A | A \in \mathrm{Mat}_{\mathbb{R}}(n,n); \det A \neq 0\}$
$\det : GL(n,\mathbb{R}) \to \mathbb{R}^* \equiv \mathbb{R}\backslash\{0\}$, det surjective homomorphism
$SL(n,\mathbb{R}) \equiv Sl_n(\mathbb{R}) = \{A | A \in \mathrm{Mat}_{\mathbb{R}}(n,n); \det A = 1\}$

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

Now

$$\mathbb{R}^* \simeq \{a1_n | a \in \mathbb{R}^*\}$$

and $\det(a1_n) = a^n$.

If n odd, and $\det(a1_n) = a^n = 1$, then $a=1$. If n even, $a = \{-1,1\}$.

By the second definition of a semi-direct product, Def. 70, it's required that $SL(n,\mathbb{R}) \cap \mathbb{R}^* = 1$ (i.e. the intersection is only the identity). This will only be the case if n odd.

cf. http://sierra.nmsu.edu/morandi/oldwebpages/math683fall2002/GroupExtensions.pdf

Part 7. Quantum Mechanics

29. The Wave function and the Schrödinger Equation, its probability interpretation, some postulates

cf. Ch. 2 "The Wave Function and the Schrödinger Equation" in **Quantum Mechanics** by Franz Schwabl (2007) [7].

From experimental considerations (Sec. 1.2.2, Schwabl (2007) [7]), with electron diffraction, electrons, e^-, have wavelike properties; let this wave be $\psi(\mathbf{x},t)$.

For free e^- of momentum $\mathbf{p}$, energy $E = \frac{\mathbf{p}^2}{2m}$, in accordance with diffraction experiments, consider as free plane waves

$$\psi(\mathbf{x},t) = C\exp\left(i(\mathbf{k}\cdot\mathbf{x} - \omega t)\right), \qquad \omega = E/\hbar = E,\, \mathbf{k} = \mathbf{p}/hbar = \mathbf{p}$$

with $\hbar = 1$

Hypothesis: wave function $\psi(\mathbf{x},t)$ gives probability distribution

$$\rho(\mathbf{x},t) = |\psi(\mathbf{x},t)|^2$$

$\rho(\mathbf{x},t)d^3x$ = probability of finding e^- at location $\mathbf{x}$ in volume element d^3x.

e.g. e^- waves $\psi_1(\mathbf{x},t)$, $\psi_2(\mathbf{x},t)$

If both slits open, superposition of wave functions $\psi_1(\mathbf{x},t) + \psi_2(\mathbf{x},t)$

Note $|\psi_1(\mathbf{x},t) + \psi_2(\mathbf{x},t)|^2 \neq |\psi_1(\mathbf{x},t)|^2 + |\psi_2(\mathbf{x},t)|^2$ if there are no interference terms.

Important remarks:

(i) Single e^- not smeared out. $\rho(\mathbf{x},t)$ is **not** the charge distribution of e^-, but is the probability density for measuring particle at position $\mathbf{x}$ at time t.
(ii) Prob. distribution doesn't occur by interference of many simultaneously incoming e^-, but one obtains same interference pattern if each e^- enters separately, i.e. even for very low intensity source. Thus, wave function applies to every electron and describes state of single e^-.

cf. 2.2 "The Schrödinger Equation for Free Particles" in **Quantum Mechanics** by Franz Schwabl (2007) [7].

(i) 1st. order DE (differential equation); (ii) linear in ψ for linear superposition (iii) "homogeneous" $\int d^3x |\psi(\mathbf{x},t)|^2 = 1$, (iv) plane waves

$$\psi(\mathbf{x},t) = C\exp\left[i(\mathbf{p}\cdot\mathbf{x} - \frac{p^2}{2m}t)/\hbar\right] \qquad \text{plane waves}$$

Should be solutions of the equations.

From postulates (i-iv),

$$i\hbar\frac{\partial}{\partial t}\psi(\mathbf{x},t) = \frac{-\hbar^2}{2m}\nabla^2\psi(\mathbf{x},t)$$

Time-dependent Schrödinger equation for free particles.

$$\int_{-\infty}^{\infty} d^3k e^{i\mathbf{k}\cdot\mathbf{x}} e^{-k^2\alpha^2} = \prod_{j=x}^{z} \int_{-\infty}^{\infty} dk_j e^{ik_jx_j} e^{-k_j^2\alpha^2} = \prod_{j=x}^{z} \left(\sqrt{\frac{\pi}{\alpha^2}} \exp\left(\frac{-x_j^2}{4\alpha^2} \right) \right) = \left(\frac{\sqrt{\pi}}{\alpha} \right)^3 \exp\left(\frac{-x^2}{4\alpha^2} \right)$$

Part 8. Algebraic Topology

cf. Bredon (1997) [12]

30. Simplicial Complexes

cf. pp. 245, from Sec. 21 Simplicial Complexes of Ch. 4 Homology Theory in Bredon (1997) [12]
$\mathbf{v}_0, \dots \mathbf{v}_n \in \mathbb{R}^\infty$, "affinely independent" if they span an affine n-plane, i.e.

$$\text{if } \left(\sum_{i=0}^n \lambda_i \mathbf{v}_i = 0, \sum_{i=0}^n \lambda_i = 0 \right), \text{ then } \Longrightarrow \forall \lambda_i = 0$$

If not, then, e.g. $\lambda_0 \neq 0$, assume $\lambda_0 = -1$, and solve the equations to get

$$\mathbf{v}_0 = \sum_{i=1}^n \lambda_i \mathbf{v}_i$$

$$\sum_{i=1}^n \lambda_i = 1$$

i.e. $\mathbf{v}_0$ is in affine space spanned by $\mathbf{v}_1 \dots \mathbf{v}_n$.
If $\mathbf{v}_0, \dots \mathbf{v}_n$ affinely independent, then

$$\sigma = (\mathbf{v}_0, \dots \mathbf{v}_n) = \{ \sum_{i=0}^n \lambda_i \mathbf{v}_i | \sum_{i=0}^n \lambda_i = 1, \, \lambda_i \geq 0 \} \tag{63}$$

is "affine simplex" spanned by $\mathbf{v}_i$; also convex hull of $\mathbf{v}_i$.
$\forall \, k \leq n$, k-face of σ is any affine simplex of form $(\mathbf{v}_{i_1}, \dots \mathbf{v}_{i_k})$, where vertices all distinct, so are affinely independent.

Definition 71. *(geometric) simplicial complex $K :=$ collection of affine simplices s.t.*

(1) $\sigma \in K \Longrightarrow$ *any face of* $\sigma \in K$*; and*
(2) $\sigma, \tau \in K \Longrightarrow \sigma \bigcap \tau$ *is a face of both* σ *and* τ*, or* $\sigma \bigcap \tau = \emptyset$

If K simplicial complex, $|K| = \bigcup \{ \sigma | \sigma \in K \} \equiv$ "polyhedron" of K

Definition 72 (Def. 21.2 of Bredon (1997) [12])**.** *polyhedron := space X if $\exists$ homeomorphism $h : |K| \xrightarrow{\approx} X$ for some simplicial complex K. h, K is triangulation of X; (map h, complex K)*

Let K finite simplicial complex.
Choose ordering of vertices $\mathbf{v}_0, \mathbf{v}_1 \dots$ of K.
If $\sigma = (\mathbf{v}_{\sigma_0}, \dots \mathbf{v}_{\sigma_n})$ is simplex of K, where $\sigma_0 < \dots < \sigma_n$, then
let $f_\sigma : \Delta_n \to |K|$ be

$$f_\sigma = [\mathbf{v}_{\sigma_b}, \dots \mathbf{v}_{\sigma_n}]$$

in notation of Def. 1.2. Bredon (1997) [12].
Then this gives CW-complex structure on $|K|$ with f_σ as characteristic maps.

Part 9. Graphs, Finite Graphs

31. Graphs, Finite Graphs, Trees

Serre (1980) [13]
cf. Chapter I. Trees and Amalgams, Section 1 Amalgams, Subsection 1.1 Direct limits of Serre (1980) [13]
Let $(G_i)_{i \in I}$, family of groups.
$\forall$ pair (i, j), let $F_{ij} =$ set of homomorphisms of G_i into G_j
Want: group $G = \varinjlim G_i$ and

$$\{ f_i | f_i : G_i \to G \} \text{s.t. } f_j \circ f = f_i \quad \forall \, f \in F_{ij}$$

group G and family $\{f_i\}$ universal in that
(*) if H group, if $\{ h_i | h_i : G_i \to H ; h_j \circ f = h_i \qquad \forall \, f \in F_{ij} \}$,
then $\exists ! h : G \to H$ s.t. $h_i = h \circ f_i$
i.e. $\mathrm{Hom}(G, H) \simeq \varprojlim \mathrm{Hom}(G_i, H)$, the inverse limit being taken relative to F_{ij}.
i.e. G direct limit of G_i relative to the F_{ij}.
EY : 20170918 this is my rewrite/reinterpretation:
Let $(G_i)_{i \in I}$, $\forall (i, j) \in I^2$, let $F_{ij} = \{ f \equiv f_{ij} | f : G_i \to G_j, f$ homomorphism of G_i into $G_j \}$.
Given group $G = \varinjlim G_i$ (for fixed i), $\{ f_i | f_i : G_i \to G | f_j \circ f = f_i \quad \forall \, f \in F_{ij} \}$, i.e.

$$\begin{tikzcd} G_i \arrow[r, "f_i"] \arrow[d, "f_{ij} \equiv f"'] & G \\ G_j \arrow[ur, "f_j"'] & \end{tikzcd}$$

Then G, $\{ f_i | f_i : G_i \to G | f_j \circ f = f_i \quad \forall \, f \in F_{ij} \}$ **universal**
if $\forall$ group H, $\forall \{ h_i | h_i : G_i \to H | h_j \circ f = h_i \quad \forall \, f \in F_{ij} \}$,

$$\begin{tikzcd} H & G_i \arrow[l, "h_i"] \arrow[r, "f_i"] \arrow[d, "f_{ij} \equiv f"] & G \arrow[ll, bend right, "\exists ! h"'] \\ & G_j \arrow[ul, "h_j"] \arrow[ur, "f_j"'] & \end{tikzcd}$$

then $\exists ! \; h : G \to H$, s.t. $h_i = h \circ f_i$ i.e.

Proposition 20. $\exists !$ *pair G, family $(f_i)_{i \in I}$, i.e. (pair consisting of $G, (f_i)_{i \in I}$, unique up to unique isomorphism.*

Proof. Define G by generators and relations.
Take generating family to be disjoint union of those for G_i.
relations - xyz^{-1} where $x, y, z \in G_i$, $z = xy \in G_i$
xy^{-1} where $x \in G_i$, $y \in G_j$, $y = f(x)$ for at least $f \in F_{ij}$.
Thus, existence of $G, \{f_i\}$.
G represents functor $H \mapsto \varprojlim \mathrm{Hom}(G_i, H)$.
Thus, uniqueness (also from universal property). ∎

e.g. groups A, G_1, G_2, homomorphisms $f_1 : A \to G_1$.
$f_2 : A \to G_2$

G obtained by amalgamating A in G_1, G_2 by $f_1, f_2 \equiv G_1 *_A G_2$.
1 can have $G = \{1\}$, even though f_1, f_2 non-trivial.

Application: (Van Kampen Thm.)

Let topological space X be covered by open U_1, U_2.
Suppose $U_1, U_2, U_{12} = U_1 \bigcap U_2$ arcwise connected.

Let basept. $x \in U_{12}$.

Then $\pi_1(X; x)$ obtained by taking 3 groups

$$\pi_1(U_1; x), \pi_1(U_2; x), \pi_1(U_{12}; x)$$

and amalagamating them according to homomorphism

$$\begin{aligned} \pi_1(U_{12}; x) &\to \pi_1(U_1; x) \\ \pi_1(U_{12}; x) &\to \pi_1(U_2; x) \end{aligned}$$

Exercise 1. Let homomorphisms $\begin{aligned} f_1 &: A \to G_1 \\ f_2 &: A \to G_2 \end{aligned}$ amalgam $G = G_1 *_A G_2$.

Define subgroups A^n, G_1^n, G_2^n, of A, G_1, G_2 recursively by

$$\begin{aligned} A^1 &= \{1\} \\ G_1^1 &= \{1\} \\ G_2^1 &= \{1\} \end{aligned}$$

$A^n =$ subgroup of A generated by $f_1^{-1}(G_1^{n-1})$ and $f_2^{-1}(G_2^{n-1})$

$$G_1^n = \text{subgroup of } G_i \text{ generated by } f_i(A^n)$$

Let A^∞, G_i^∞ be unions of A^n, G_i^n resp.

Show that f_i defines injection $A/A^\infty \to G_i/G_i^\infty$.

So the amalgamation is $G \simeq G_1/G_1^\infty *_{A/A^\infty} G_2/G_2^\infty$.

Take the first induction case (for intuition about the solution).

$$\begin{aligned} A^2 &= \langle f_1^{-1}(G_1^1), f_2^{-1}(G_2^1) \rangle = \langle f_1^{-1}(\{1\}), f_2^{-1}(\{1\}) \rangle \\ G_i^2 &= f_i(A^2) \end{aligned}$$

Let $f_i(a) = f_i(b) \in G_i/G_i^\infty$; $a, b \in A/A^\infty$.

Then since $f_i(a), f_i(b) \in G_i/G_i^\infty$, $f_i(a), f_i(b) \in \{gG_i^\infty | g \in G_i\}$ (quotient is defined to be the set of all left cosets of G_i^∞, which has to be a normal subgroup for G_i/G_i^∞ to be a quotient group).

Since $a, b \in A/A^\infty$, suppose we take $a, b \in A$.

And suppose we take

$$\begin{aligned} f_i(a) &= f_i(a)G_i^\infty = f_i(a)f_i(A^{n_a}) = f_i(aA^{n_a}) \\ f_i(b) &= f_i(b)G_i^\infty = f_i(b)f_i(A^{n_b}) = f_i(bA^{n_b}) \end{aligned}$$

Taking f_i^{-1} (recall for group homomorphisms, they map inverse of element of 1st. group to inverse of image of this element).

$aA^{n_a} = bA^{n_b} \in A/A^\infty$ (This is okay as we've "quotiented out A^∞; so indeed, they're equal)

cf. Subsection 1.2 Structure of amalgams of Serre (1980) [13]

Suppose given group A, family of groups $(G_i)_{i \in I}$, and, $\forall i \in I$, injective homomorphism $A \to G_i$.

$*_A G_i \equiv$ direct limit (cf. no. 1.1) of family (A, G_i) with respect to these homomorphisms, call it *sum* (in category theory sense, i.e. product) of G_i with A amalgamated.

e.g. $A = \{1\}$,
$*G_i \equiv$ free product of G_i.

31.0.1. *reduced word.* $\forall i \in I$, choose set S_i of right coset representations of G_i modulo A, assume $1 \in S_i$,

$(a, s) \mapsto as$ is bijection of $A \times S_i$ onto G_i,
$A \times (S_i - \{1\}) \to G_i - A$ (onto)

Let $\mathbf{i} = (i_1 \dots i_n)$, $n \geq 0$, $i_j \in I$, s.t.

$$i_m \neq i_{m+1} \text{ for } 1 \leq m \leq n-1 \tag{64}$$

cf. (T) of Serre (1980) [13].

So *reduced word* m is defined as

$$m = (a; s_1 \dots s_n)$$

where $a \in A, s_1 \in S_{i_1} \dots s_n \in S_{i_n}$, and $s - j \neq 1 \forall j$.

$f \equiv$ canonical homomorphism of A into group $G = *_A G_i$
$f_i \equiv$ canonical homomorphism of G_i into group $G = *_A G_i$

EY : 20170611 (Further explanations, basic examples, from me):

Given $A, \{G_i\}_{i \in I}$, injective (group) homomorphisms $\{f_i : A \to G_i\}_i$.

$G_i \backslash f_i(A) = \{f_i(A)g | g \in G_i\}$.

Right coset representation of $f_i(A)g \mapsto g$.

e.g. A, G_1, G_2, $\begin{aligned} f_1 &: A \to G_1. \\ f_2 &: A \to G_2 \end{aligned}$

$$\begin{aligned} G_1 \backslash f_1(A) &= \{f_1(A)g | g \in G_1\} \\ G_2 \backslash f_2(A) &= \{f_2(A)g | g \in G_2\} \end{aligned}$$

$\mathbf{i} = (i_1 \dots i_n)$, $i_j \in I$, $i_m \neq i_{m+1}$ for $1 \leq m \leq n-1$.

Consider $(1212 \dots 12)$

$m = (a; f_1 g_2 f_3 g_4 \dots f_{2n-1}, g_{2n})$ where f's $\in S_1 \subset G_1$, g's $\in S_2 \subset G_2$.

and so

Definition 73 (reduced word)**.** ***reduced word*** *of type* $\mathbf{i}$, m,

$$m = (a; s_1 \dots s_n) \tag{65}$$

where $a \in A, s_1 \in S_{i_1}, \dots s_n \in S_{i_n}$, $s_j \neq 1 \quad \forall j$,
$\mathbf{i} = (i_1 \dots i_n)$, $i_j \in I$, *s.t.* $i_m \neq i_{m+1}$ *for* $1 \leq m \leq n-1$,
with $S_i = \{g | g \in f_i(A)g \in f_i(A)G_i\}$

Theorem 14 (1 of Serre (1980) [13])**.** *$\forall g \in G$, $\exists$ sequence $\mathbf{i}$ s.t. $i_m \neq i_{m+1}$ for $1 \leq m \leq n-1$ and reduced word*

$$m = (a; s_1 \dots s_n)$$

of type $\mathbf{i}$ *s.t.*

$$g = f(a) f_{i_1}(s_1) \dots f_{i_n}(s_n)$$

Furthermore, $\mathbf{i}$ and m unique.

Remark. Thm. 1 implies $f; f_i$ injective.

Then identify A and G_i with images $f(A), f_i(G_i)$ in G, and reduced decomposition (*) of $g \in G$

$$g = as_1 \dots s_n, \quad a \in A, \; s_1 \in S_{i_1} - \{1\} \dots s_n \in S_{i_n} - \{1\}$$

Likewise, $G_i \bigcap G_j = A$ if $i \neq j$.

In particular, $S_i - \{1\}$ pairwise disjoint in G.

Proof. Let $X_i \equiv$set of reduced words of type $\mathbf{i}$, $X = \coprod X_i$.
Make G act on X.
In view of universal property of G, sufficient to make $\forall\, i, G_i$ act,
check action induced on A doesn't depend on i
Suppose then that $i \in I$, and let $Y_i =$ set of reduced words of form $(1; s_1 \dots s_n)$, with $i_1 \neq i$.
EY : 20170611
Recall that

$$S_i = \{ g | g \in f_i(A) g \in f_i(A) G_i \}$$

$$\begin{aligned} & A \times S_i \to G_i \text{ onto} \\ & A \times (S_i - \{1\}) \to G_i - A \text{ onto} \\ & (a,s) \mapsto as \text{ bijection} \end{aligned}$$

Let $Y_i =$ set of reduced words of form $(1; s_1 \dots s_n) = \{ (1; s_1 \dots s_n) | 1 \in A; s_1 \in S_{i_1} \dots s_n \in S_{i_n}; \mathbf{i} = (i_1 \dots i_n), i_j \in I \text{ s.t. } i_m \neq i_{m+1} \text{ for } 1 \leq m \leq n-1 \}$.

$$\begin{gathered} A \times Y_i \to X = \coprod_i X_i \\ (a, (1; s_1 \dots s_n)) \mapsto (a; s_1 \dots s_n) \\ A \times \{ S_i - \{1\} \} \times Y_i \to X \\ ((a,s), (1; s_1 \dots s_n)) \mapsto (a; s, s_1 \dots s_n) \end{gathered}$$

and remember that $X_i =$ set of reduced words of type $\mathbf{i}$.
It's clear that this yields a bijection $A \times Y_i \bigcup A \times (S_i - \{1\}) \times Y_i \to X$.
Let $x \in X$. Then $x \in X_{\mathbf{i}}$ for some $\mathbf{i}$. So x is a reduced word of type $\mathbf{i}$: $x = (a; s_1 \dots s_n)$. Then clearly $x = (a; s_1 \dots s_n) \mapsto (a, (1; s_1 \dots s_n)) \in A \times Y_i$.

□

cf. pp. 13, Sec. 2. Trees, 2.1 Graphs of Serre (1980) [13]

Definition 74 (1. of Serre (1980) [13])**.** ***graph*** $\Gamma = (X, Y, Y \to X \times X, Y \to Y)$, *where* $\begin{aligned} \text{set } X = & \ \text{vert}\,\Gamma \\ \text{set } Y = & \ \text{edge}\,\Gamma \end{aligned}$

$$\begin{aligned} & Y \to X \times X \\ & y \mapsto (o(y), t(y)) \\ & Y \to Y \\ & y \mapsto \overline{y} \end{aligned}$$

s.t. $\forall\, y \in Y$, $\overline{\overline{y}} = y$, $\overline{y} \neq y$, $o(y) = t(\overline{y})$.
vertex $P \in X$ *of* Γ.
(oriented) edge $y \in Y$, $\overline{y} \equiv$ *inverse edge.*
origin of $y :=$ *vertex* $o(y) = t(\overline{y})$.
terminus of $y :=$ *vertex* $t(y) = o(\overline{y})$
extremities of $y := \{o(y), t(y)\}$
If 2 vertices ***adjacent****, they're extremities of some edge.*
orientation of graph $\Gamma = Y_+ \subset Y =$ *edge* Γ *s.t.* $Y = Y_+ \coprod \overline{Y}_+$*. It always exists.*
oriented graph defined, up to isomorphism, by giving 2 sets X, Y_+ *and* $Y+ \to X \times X$*.*
corresponding set of edges is $Y = Y_+ \coprod \overline{Y}_+$ *where* $\overline{Y}_+ \equiv$ *copy of* Y_+

31.0.2. *Realization of a Graph.* cf. Realization of a Graph in Serre (1980) [13].
Let graph Γ, $X = \text{vert}\Gamma$, $Y = \text{edge}\Gamma$.
topological space $T = X \coprod Y \times [0,1]$, where X, Y provided with discrete topology.
Let R be finest equivalence relation on T for which

$$\begin{aligned} & (y,t) \equiv (\overline{y}, 1-t) \\ & (y,0) \equiv o(y) \qquad \forall\, y \in Y, \forall\, t \in [0,1] \\ & (y,1) \equiv t(y) \end{aligned} \tag{66}$$

quotient space real$(\Gamma) = T/R$ is *realization* of graph Γ. (realization is a functor which commutes with direct limits).
Let $n \in \mathbb{Z}^+$. Consider oriented graph of $n+1$ vertices $0, 1, \dots n$,

Definition 75. *path (of length* n*) in graph* Γ *is morphism* c *of* $Path_n$ *into* Γ

orientation given by n edges $[i, i+1]$, $0 \leq i < n$, $\begin{aligned} o([i,i+1]) = i \\ t([i,i+1]) = i+1 \end{aligned}$
For $n \geq 1$,
$(y_1 \dots y_n)$ sequence of edges $y_i = c([i-1, i])$ s.t.

$$t(y_i) = o(y_{i+1}), \qquad 1 \leq i < n \text{ determine } c$$

If $P_i = c(i)$,
c is a path from P_0 to P_n, and P_0 and P_n are *extremities of the path c.*
pair of form $(y_i, y_{i+1}) = (y_i, \overline{y}_i)$ in path is **backtracking**.
path (of length $n-2$), from P_0 to P_n given (for $n > 2$) by $(y_1 \dots y_{i-1}, y_{i+2} \dots y_n)$
If $\exists$ path from P to Q in Γ, $\exists$ one without backtracking (by induction)
direct limit $\text{Path}_\infty = \varinjlim \text{Path}_n$ provides notion of infinite path.
$\text{Path}_\infty \ni$ infinite sequence $(y_1, y_2, \dots)$ of edges s.t. $t(y_i) = o(y_{i+1}) \quad \forall\, i \geq 1$.

Definition 76 (connected graph; Def. 3 of Serre (1980) [13])**.** *graph connected if* $\forall$ *2 vertices, 2 vertices are extremities of at least 1 path.*
maximal connected subgraphs (under relation of inclusion) are connected components *of graph.*

31.0.3. *Circuits.* Let $n \in \mathbb{Z}^+$, $n \geq 1$.
Consider

set of vertices $\mathbb{Z}/n\mathbb{Z}$, orientation given by n edges $[i, i+1]$, $(i \in \mathbb{Z}/n\mathbb{Z})$ with $\begin{aligned} o([i,i+1]) = i \\ t([i,i+1]) = i+1 \end{aligned}$

Definition 77 (circuit; Def. 4 of Serre (1980) [13])**.** *circuit (length* n*) in graph is subgraph isormorphic to* $Circ_n$*.*

i.e. subgraph = path $(y_1 \dots y_n)$, without backtracking, s.t. $P_i = t(y_i)$, $(1 \leq i \leq n)$ distinct, s.t. $P_n = o(y_1)$

$n = 1$ case: Circ_1, $\mathbb{Z}/\mathbb{Z} = \{0\}$, 1 edge, $[0,1]$, $0 \in \mathbb{Z}/1\mathbb{Z}$, $\begin{aligned} o([0,1]) = 0 \\ t([0,1]) = 1 \end{aligned}$
Note Circ_1 has automorphism of order 2, which changes its orientation, i.e.
$\exists$ automorphism $\sigma \in \text{Aut}(\text{Circ}_1)$ s.t. $|\sigma| = 2$, i.e. $\sigma^2 = 1$.
loop := circuit of length 1; so loop $\in \overline{\text{Circ}_1}$.
path (y_1), $P_1 = t(y_1) = o(y_1)$.

$n=2$ case: Circ_2, $\mathbb{Z}/2\mathbb{Z} = \{0,1\}$, 2 edges $[0,1], [1,2]$,

path (y_1, y_2), $(1 \leq i \leq 2)$,
$$P_1 = t(y_1)$$
$$P_2 = t(y_2) = o(y_1)$$

31.1. **Combinatorial graphs.** Let $(X,S) \equiv$ simplicial complex of dim. ≤ 1, with
$X \equiv$ set
$S \equiv$ set of subsets of X with 1 or 2 elements, containing all the 1-element subsets.
associates with it a graph $\Gamma = (X, \{(P,Q)\})$.
X is its set of vertices.
edges $= \{(P,Q) \in X \times X\}$ s.t. $P \neq Q$, $\{P,Q\} \in S$, with $\overline{(P,Q)} = (Q,P)$
$$o(P,Q) = P$$
$$t(P,Q) = Q$$

In this graph, 2 edges with same origin and same terminus are equal. This is equivalent to (see following Def.)

Definition 78 (combinatorial; Def. 5 of Serre (1980) [13]). *graph is combinatorial if it has no circuit of length* ≤ 2

Conversely, it's easy to see that
every combinatorial graph Γ derived (up to isomorphism) by construction above from simplicial complex (X,S), where
$X = \text{vert}\Gamma$
$S =$ set of subset $\{P,Q\}$ of X s.t. P and Q either adjacent or equal.

Part 10. Tensors, Tensor networks; Singular Value Decomposition, QR decomposition, Density Matrix Renormalization Group (DMRG), Matrix Product states (MPS)

32. Introductions to Tensor Networks

José Barbon (IFT-CSIC, Univ. Autonoma de Madrid) gave the https://youtu.be/nsxgAOAEgbg for the workshop "Black Holes, Quantum Information, Entanglement, and all that," (29 May-1 June, 2017, with the organizing committee of Thibault Damour (IHES), Vasily Pestun (IHES), Eliezer Rabinovici (IHES & Hebrew Univ. of Jerusalem).

In the talk,
cf. 43:13

The church of the doubled Hilbert space. Any thermal box can be obtained by tracing over a second identical copy, if appropriately entangled into a global pure state.

$$\rho_R = \text{Tr}_L \sum_n C_n \Psi_n^L \otimes \Psi_n^R$$
$$(C_n)_{\text{thermal}} = \left[\frac{e^{-\beta E_n}}{\sum_m e^{-\beta E_M}} \right]^{1/2}$$

But!!
If the entanglement basis is taken to be the high-energy band of two "entangled" CFTs ...
$$|TFD\rangle \sim \sum_{E_n} e^{-\beta E_n/2} |E_n\rangle_L \otimes |E_n\rangle_R$$
neglecting the tiny e^{-S} spacings. we can approximate by continuous spectrum of fields in the background of an AdS black hole, to get ...

$$\int_E e^{-\beta E/2} |E\rangle_L \otimes |E\rangle_R$$

The HH state of the bulk fields!

cf. 46:16
SLOGAN: EPR = ER Maldacena-Susskind
Accumulating a density of entanglement of $S \gg 1$ well-separated Bell pairs within a transversal size of order $(GS)^{1/2}$ seems to generate a geometrical bridge of area GS.
cf. 49:26

Parametrizing complexity of entanglement. Pick a tensor decomposition of Hilbert space of dimension $\exp(S)$ into S factors of $O(1)$ dimension.
$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_S$$
A tensor of S indices gives a generic state.
cf. 50:27
The decomposition of the big tensor in small building blocks gives a notion of "complexity of entanglement"
rather simple entanglement pattern
somewhat more complex entanglement pattern
picture from M von Raamsdonk
cf. 55:10

A list of open questions & problems.

- Need exactly calculable toy models of AdS/CFT along the lines of SYK model
- Give a "renormalized" definition of quantum complexity for continuum CFTs
- Can tensor networks describe bulk gravitons?
- What is the space-time meaning of quantum complexity saturation?
- Can we define approximate local observables for black hole inferiors?
- Are there obstructions related to firewalls and/or fuzzballs?

Workshop introductory overview by José Barbon for the Institut des Hautes Études Scientifiques (IHÉS) gave me the first impetus to understand tensor networks as I sought to also understand the condensates of entanglement pairs within the black hole.

A Google search for introductions to tensor networks that are on arxiv ("Introduction Tensor Network arxiv") yielded Bridgeman and Chubb's course notes (bf. Bridgeman and Chubb (2017) [17]).

32.1. List of stuff I want to look at/do/study.

I would like to compare/contrast the following:

- Rotman (2010) [14], Ch. 8, but starting from 8.4 Tensor Products, pp. 574
- Jeffrey Lee (2009) [16], Ch. 7 Tensors
- `http://www.irisa.fr/sage/bernard/publis/SVD-Chapter06.pdf`, `https://math.stackexchange.com/questions/694339/parallel-algorithms-for-svd`

Maldacena and Susskind (2013) [22]
Lectures on Gravity and Entanglement. Mark Van Raamsdonk [25]

- Consider as physical system AdS-Schwarzchild black hole
- CFT
  - PFL Lectures on Conformal Field Theory in $D \geq 3$ Dimensions, Rychkov (2016) [23].

Evenbly and Vidal (2011) [24], Tensor network states and geometry
Loose ends (might not be useful links)

- `https://arxiv.org/pdf/1506.06958.pdf`
- `https://arxiv.org/pdf/1512.02532.pdf` One-point Functions in AdS/dCFT from Matrix Product States

Numerical implementation strategy: 1st, CUDA cuSolver, 2nd, Numerical Recepes version, 3rd, parallel algorithm review.

32.2. Tensor operations; Tensor properties.

32.2.1. *rank.* $r =$ rank tensor of dim. $d_1 \times \dots \times d_r$ is element of $\mathbb{C}^{d_1 \times \dots \times d_r}$

Tensor product

$$[A \otimes B]_{i_1 \dots i_r, j_1 \dots j_s} := A_{i_1 \dots i_r} \cdot B_{j_1 \dots j_s} \tag{67}$$

32.2.2. *Trace.* Given tensor A, xth, yth indices have identical dims. ($d_x = d_y$), partial trace over these 2 dims. is simply joint summation over that index

$$[\mathrm{Tr}_{x,y} A]_{i_1 \dots i_{x-1} i_{x+1} \dots i_{y-1} i_{y+1} \dots i_r} = \sum_{\alpha=1}^{d_x} A_{i_1 \dots i_{x-1} \alpha i_{x+1} \dots i_{y-1} \alpha i_{y+1} \dots i_r} \tag{68}$$

32.2.3. *Contraction.*

32.2.4. *Group and splitting, Bridgeman and Chubb (2017)* [17]. "Rank is a rather fluid concept in the study of tensor networks." Bridgeman and Chubb (2017) [17].

$\mathbb{C}^{a_1 \times \dots \times a_n} \simeq \mathbb{C}^{b_1 \times \dots \times b_m}$ isomorphic as vector spaces if $\prod_i a_i = \prod_i b_i$.

We can "group" or "split" indices to lower or raise rank of given tensor, resp.

Consider contracting 2 arbitrary tensors.

If we group together indices which are and are not involved in contraction,

"It should be noted that not only is this reduction to matrix multiplication pedagogically handy, but this is precisely the manner in which numerical tensor packages perform contraction, allowing them to leverage highly optimised matrix multiplication code." (cf. Bridgeman and Chubb (2017) [17]; check this)

"Owing to freedom in choice of basis, precise details of grouping and splitting aren't unique." (cf. Bridgeman and Chubb (2017) [17]).

1 specific choice of convention:

tensor product basis, defining basis on product space by product of respective bases.

"The canonical use of tensor product bases in quantum information allows for grouping and splitting described above to be - dealt with implicitly."

$$|0\rangle \otimes |1\rangle \equiv |0\rangle \tag{69}$$

and precisely this grouping,

$$\begin{gathered} |0\rangle \otimes |1\rangle \in \mathrm{Mat}_{\mathbb{C}}(2,2), \text{ whilst} \\ |01\rangle \in \mathbb{C}^4 \end{gathered} \tag{70}$$

Suppose rank $n+m$ tensor T, group its first n indices, last m indices together.

$$T_{I,J} := T_{i_1 \dots i_n, j_1 \dots j_m}$$

where

$$\begin{aligned} I &:= i_1 + d_1^{(i)} i_2 + d_1^{(i)} d_2^{(i)} i_3 + \dots + d_1^{(i)} \dots d_{n-1}^{(i)} i_n \\ J &:= j_1 + d_1^{(j)} j_2 + d_1^{(j)} d_2^{(j)} j_3 + \dots + d_1^{(j)} \dots d_{m-1}^{j)} j_m \end{aligned}$$

EY : 20170627 to elaborate, consider a functor `flatten` that does what's described above, in the context of category theory (and so this is the generalization):

$$\begin{gathered} \mathbb{K}^{d_1^{(i)}} \times \mathbb{K}^{d_2^{(i)}} \times \dots \times \mathbb{K}^{d_n^{(i)}} \times \mathbb{K}^{d_1^{(j)}} \times \mathbb{K}^{d_2^{(j)}} \times \dots \times \mathbb{K}^{d_m^{(j)}} \xrightarrow{\text{flatten}} \mathbb{K}^{\prod_{p=1}^n d_p^{(i)}} \times \mathbb{K}^{\prod_{q=1}^m d_q^{(j)}} \\ T_{i_1 \dots i_n, j_1 \dots j_m} \xmapsto{\text{flatten}} T_{I,J} \\ \{0,1,\dots d_1^{(i)}\} \times \{0,1,\dots d_2^{(i)}\} \times \dots \times \{0,1,\dots d_n^{(i)}\} \times \{0,1,\dots d_1^{(j)}\} \times \{0,1,\dots d_2^{(j)}\} \times \dots \times \{0,1,\dots d_m^{(j)}\} \xrightarrow{\text{flatten}} \\ \xrightarrow{\text{flatten}} \{0,1,\dots \prod_{p=1}^n d_p^{(i)} - 1\} \times \{0,1,\dots \prod_{q=1}^m d_q^{(j)} - 1\} \\ (i_1, i_2, \dots i_n, j_1, j_2 \dots j_m) \xmapsto{\text{flatten}} (I,J) := (i_1 + d_1^{(i)} i_2 + \dots + d_1^{(i)} \dots d_{n-1}^{(i)} i_n, j_1 + d_1^{(j)} j_2 + \dots + d_1^{(j)} \dots d_{m-1}^{(j)} j_m) \end{gathered} \tag{71}$$

It doesn't make sense to call this "row-major" or "column-major" ordering generalization, because we are not dealing with only 2 indices where we can definitely say the first index indexes the "row" and the second index indexes the "column." At most, possibly, you can alternatively have this:

$$(i_1 \dots i_n, j_1 \dots j_m) \xmapsto{\text{flatten}} (I,J) := (d_2^{(i)} \dots d_n^{(i)} i_1 + d_3^{(i)} \dots d_n^{(i)} i_2 + \dots + i_n, d_2^{(j)} \dots d_m^{(j)} j_1 + \dots + j_m)$$

Note that this is all 0-*based counting* (i.e. we start counting from 0 just like in C,C++,Python, etc.). If you really wanted 1-based counting, you'd have to complicate the above formulas as such:

$$(I,J) := (i_1 + d_1^{(i)}(i_2 - 1) + \dots + d_1^{(i)} \dots d_{n-1}^{(i)}(i_n - 1), j_1 + d_1^{(j)}(j_2 - 1) + \dots + d_1^{(j)} \dots d_{m-1}^{(j)}(j_m - 1))$$

Note that formulas are easily checked by pluggin in the minimum and maximum values for the indices and seeing if they make sense (e.g. plug in $(0,0,\dots,0)$ for all indices for 0-based counting and make sure you get back $I = 0$ or $J = 0$).

32.3. **Singular Value Decomposition.**

$$\begin{gathered} T_{I,J} = \sum_\alpha U_{I,\alpha} S_{\alpha,\alpha} \overline{V}_{J,\alpha} \\ \mathrm{Mat}_{\mathbb{K}}(N,M) \xrightarrow{\text{SVD}} \mathrm{Mat}_{\mathbb{K}}(N,P) \times \mathrm{Mat}_{\mathbb{K}}(P,P) \times \mathrm{Mat}_{\mathbb{K}}(M,P) \\ T_{I,J} \xmapsto{\text{SVD}} U_{I,\alpha}, S_{\alpha,\alpha}, \overline{V}_{I,\alpha} \text{ s.t.} \\ T_{I,J} = \sum_\alpha U_{I,\alpha} S_{\alpha,\alpha} \overline{V}_{J,\alpha} \\ T = USV^\dagger \end{gathered} \tag{72}$$

For the higher-dimensional version of SVD,

$$\begin{gathered} \mathbb{K}^{d_1^{(i)}} \otimes \dots \otimes \mathbb{K}^{d_N^{(i)}} \otimes \mathbb{K}^{d_1^{(j)}} \otimes \dots \otimes \mathbb{K}^{d_M^{(j)}} \xrightarrow{\text{flatten}} \mathrm{Mat}_{\mathbb{K}}(N,M) \xrightarrow{\text{SVD}} \mathrm{Mat}_{\mathbb{K}}(N,P) \times \mathrm{Mat}_{\mathbb{K}}(P,P) \times \mathrm{Mat}_{\mathbb{K}}(M,P) \xrightarrow{\text{splitting}} \\ \xrightarrow{\text{splitting}} \mathbb{K}^{d_1^{(i)}} \otimes \dots \otimes \mathbb{K}^{d_N^{(i)}} \otimes \mathbb{K}^P \times \mathrm{Mat}_{\mathbb{K}}(P,P) \times \mathbb{K}^{d_1^{(j)}} \otimes \dots \otimes \mathbb{K}^{d_M^{(j)}} \otimes \mathbb{K}^P \\ T_{i_1 \dots i_N, j_1 \dots j_M} = \sum_\alpha U_{i_1 \dots i_N, \alpha} S_{\alpha,\alpha} \overline{V}_{j_1 \dots j_M, \alpha} \end{gathered} \tag{73}$$

33. Density Matrix Renormalization Group; Matrix Product States (MPS)

33.1. **Introduction; physical system (physical setup).** cf. "Density Matrix Renormalization Group/Matrix Product States" lectures by Schollwöck (2017) [20].

Recall the fundamental Hamiltonian (frequently in solid state physics), for *electrons moving in a Hamiltonian potential.*

$$H = \sum_{j=1}^{e^-} \frac{\mathbf{p}_j^2}{2m_e} + \frac{1}{2} \frac{1}{4\pi\epsilon_0} \frac{q_e^2}{|\mathbf{r}_i - \mathbf{r}_j|^2} + \sum_{j=1}^{e^-} V_{\text{eff}}(\mathbf{r}_j) \tag{74}$$

where $\frac{\mathbf{p}_j^2}{2m_e}$ is the kinetic energy term, $\sum_{j=1}^{e^-} V_{\text{eff}}(\mathbf{r}_j)$ is the lattice potential. The problem is in the 2nd. term, electron-electron interaction, $\frac{1}{2}\frac{1}{4\pi\epsilon_0}\frac{q_e^2}{|\mathbf{r}_i-\mathbf{r}_j|^2}$

Typical models include the following:

- Hubbard model (tight, binding-like model; basis states are not energy states but *Wannier basis* states):

$$H = -t\sum_{\langle i,j\rangle,\sigma} c^\dagger_{i\sigma}c_{j\sigma} + h.c. + U\sum_i n_{i\uparrow}n_{i\downarrow} \tag{75}$$

where $\langle i,j\rangle$ denotes nearest neighbors, σ index is for all possible states, $h.c.$ stands for hermitian conjugate, and $d \equiv$ number of states of single spin site.

$-t\sum_{\langle i,j\rangle,\sigma} c^\dagger_{i\sigma}c_{j\sigma} + h.c.$ is the kinetic energy term,

$U\sum_i n_{i\uparrow}n_{i\downarrow}$ is the Coulomb energy.

Hilbert space for the Hubbard model is

$$\{|\emptyset\rangle, |\uparrow\rangle, |\downarrow\rangle, |\uparrow\downarrow\rangle\}^{\otimes L}, \qquad d=4 \tag{76}$$

- Heisenberg model (large -U Hubbard at half-filling)

$$H = J\sum_{\langle i,j\rangle}\mathbf{S}_i\cdot\mathbf{S}_j = J\sum_{\langle i,j\rangle}\frac{1}{2}(S_i^+S_j^- + S_j^+S_i^-) + S_i^zS_j^z) \tag{77}$$

Hilbert space $\{|\uparrow\rangle, |\downarrow\rangle\}^{\otimes L}$, $d=2$

33.1.1. *Compression of information viewpoint for solid-state Hamiltonians, quantum many-body systems.* .

"emergent" macroscopic quantities, τ, p (temperature, pressure). For

$$H = J\sum_{\langle i,j\rangle}\mathbf{S}_i\cdot\mathbf{S}_j = J\sum_{\langle i,j\rangle}\frac{1}{2}(S_i^+S_j^- + S_j^+S_i^-) + S_i^zS_j^z)$$

H as classical spins: thermodynamic limit $N\to\infty$. 2 angles required to describe unit vector on unit sphere $(S^3) \implies 2N$ degrees of freedom (linear)

quantum spins: superposition of states, thermodynamic limit: $N\to\infty$, 2^N degrees of freedom (exponential).

33.1.2. *Definitions; notation and conventions.* Quantum system living on L lattice sites; cf. Schollwöck (2017) [20], lattice can be in any dim., effectively most useful in 1-dim., think of the example of a 1-dim. chain of L sites.

d local states per site $\{\sigma_i\}$, $i\in\{1,2,\dots L\}$

e.g. spin $\frac{1}{2}$, $d=2$, $|\uparrow\rangle, |\downarrow\rangle$.

Hilbert space: $\mathcal{H} = \otimes_{i=1}^L \mathcal{H}_i$, $\mathcal{H}_i = \{|1_i\rangle, \dots |d_i\rangle\}$.

Notice, there are *exponentially many coefficients*, c's. Most general state (not necessarily 1-dim.) is

$$|\psi\rangle = \sum_{\sigma_1\dots\sigma_L} c^{\sigma_1\dots\sigma_L}|\sigma_1\dots\sigma_L\rangle \tag{78}$$

abbreviations: $\{\sigma\} = \sigma_1\dots\sigma_L$. And so we can write $c^{\{\sigma\}}$.

33.2. **MPS, matrix product states.**

$$|\psi\rangle = \sum_{\sigma_1\dots\sigma_L} M^{\sigma_1}M^{\sigma_2}\dots M^{\sigma_L}|\sigma_1\sigma_2\dots\sigma_L\rangle \tag{79}$$

The $\sum_{\sigma_1\dots\sigma_L}$ means that all basis states participate; Schollwöck is not kicking out any states arbitrarily.

$$c^{\{\sigma\}} = M^{\sigma_1}M^{\sigma_2}\dots M^{\sigma_L} \in \mathbb{C}$$

so

$M^{\sigma_1} \in \text{Mat}_{\mathbb{C}}(1, n_1)$ so to get a scalar in the product of matrices. Likewise, $M^{\sigma_L} \in \text{Mat}_{\mathbb{C}}(m_L, 1)$ (variational) constraint is in expansion coefficients.

$\forall$ d local basis states, $|\sigma_i\rangle \in V_i \equiv V$,$\dim V = d$, let there be 1 matrix M, i.e. M^{σ_i}.

Thus, dL matrices altogether (in total).

Assume matrix size has upper limit D (a computer limitation).

Up to dLD^2 coefficients, instead of exponentially many ($c^{\{\sigma\}}$, and sum over $\{\sigma\}$).

33.2.1. *Product States and MPS.* Mean-filed approximation/product state misses essential quantum feature: **entanglement**.

Consider 2 spin $\frac{1}{2}$ systems: $\mathcal{H} = \mathcal{H}_1\otimes\mathcal{H}_2$, $\mathcal{H}_i = \{|\uparrow\rangle, |\downarrow\rangle\}$

General state is

$$|\psi\rangle = c^{\uparrow\uparrow}|\uparrow\uparrow\rangle + c^{\uparrow\downarrow}|\uparrow\downarrow\rangle + c^{\downarrow\uparrow}|\downarrow\uparrow\rangle + c^{\downarrow\downarrow}|\downarrow\downarrow\rangle$$

e.g. singlet state: $|\psi\rangle = \frac{1}{\sqrt{2}}|\uparrow\downarrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\uparrow\rangle$.

As an exercise, show that the singlet state cannot be written as product of local coefficients, i.e.

$$c_{\uparrow\downarrow} \neq c^{\uparrow}c^{\downarrow}$$

Instead of writing products of scalars, write product of matrices, i.e. $e^{\sigma_1}\cdot e^{\sigma_2} \to M^{\sigma_1}M^{\sigma_2}$

$$M^{\uparrow 1} = \begin{bmatrix}1 & 0\end{bmatrix} \quad M^{\downarrow 1} = \begin{bmatrix}0 & 1\end{bmatrix} \quad \begin{matrix} M^{\uparrow 2} = \begin{bmatrix}0 \\ \frac{-1}{\sqrt{2}}\end{bmatrix} \\ M^{\downarrow 2} = \begin{bmatrix}\frac{1}{\sqrt{2}} \\ 0\end{bmatrix}\end{matrix}$$

$$M^{\uparrow 1}M^{\downarrow 2} = \frac{1}{\sqrt{2}}$$
$$M^{\downarrow 1}M^{\uparrow 2} = \frac{-1}{\sqrt{2}}$$

33.2.2. *AKLT model (Affleck-Kennedy-Lieb-Tasaki).* MPS is useful even for matrices of dim. 2.

33.3. **General matrix product state (MPS) and SVD (Singular Value Decomposition).** cf. Schollwöck (2017) [20]

The general matrix product state (MPS) is the following:

$$|\psi\rangle = \sum_{\sigma_1\dots\sigma_L} M^{\sigma_1}M^{\sigma_2}\dots M^{\sigma_L}|\sigma_1\sigma_2\dots\sigma_L\rangle \tag{80}$$

where $\sigma_i \in V_i$, $\dim V_i = d_i$ and

$M^{\sigma_1} \in \text{Mat}_{\mathbb{C}}(1, D_1)$

$M^{\sigma_2} \in \text{Mat}_{\mathbb{C}}(D_1, D_2)$

$\vdots$

$M^{\sigma_{L-1}} \in \text{Mat}_{\mathbb{C}}(D_{L-2}, D_{L-1})$

$M^{\sigma_L} \in \text{Mat}_{\mathbb{C}}(D_{L-1}, 1)$

Notice the non-unique **gauge degree of freedom**:

$\forall A \in \text{Mat}_{\mathbb{C}}(m,n)$, then for $k = \min(m,n)$,

$$A = USV^\dagger \equiv U\Sigma V^\dagger \text{ where} \tag{81}$$

$U \in \text{Mat}_{\mathbb{C}}(m,k)$, $U^\dagger U = 1$ (i.e. U consists of orthonormal columns, or k number of u's $\in \mathbb{C}^m$); if $m=k$, $UU^\dagger = 1$,

$S \in \text{Mat}_{\mathbb{C}}(k,k)$ s.t. $S \in \text{diag}_{\mathbb{C}}(k)$, $s_1 \geq s_2 \geq s_3 \geq \dots s_i \geq 0$, s_j's non-negative "singular values" (adjacent "singular" in name doesn't imply anything), non-vanishing = rank$r \leq k$.

$V^\dagger \in \text{Mat}_{\mathbb{C}}(k,n)$, $V^\dagger V = 1$, (orthonormal rows, or k number of $v \in \mathbb{C}^n$); if $k=n$, $VV^\dagger = 1$

Recall eigenvalue equation and thus so-called eigenvalue decomposition.

For $A \in \text{Mat}_{\mathbb{C}}(m,m)$,

$$\begin{gathered} Au_j = \lambda_j u_j; \qquad j = 1\dots r;\ r \equiv \text{ rank }, \quad u_j \in \text{Mat}_{\mathbb{C}}(m,1) \\ A_{ik}u_{kj} = \lambda_j u_{ij} = u_{ik}\delta_{kj}\lambda_j \Longrightarrow AU = U\Lambda \end{gathered}$$

with $U \in \text{Mat}_{\mathbb{C}}(m,r)$, $\Lambda \in \text{Mat}_{\mathbb{C}}(r,r)$.

And so

$$\begin{gathered} AA^\dagger = USV^\dagger VSU^\dagger = US^2U^\dagger \Longrightarrow (AA^\dagger)U = US^2 \\ A^\dagger A = VSU^\dagger USV^\dagger = VS^2V^\dagger \Longrightarrow (A^\dagger A)V = VS^2 \end{gathered}$$

so if we treat U and V, matrices of left, right singular vectors, then S^2 singular value squared are eigenvalues.

Start with

$$|\psi\rangle = \sum_{\sigma_1\dots\sigma_L} c^{\sigma_1\dots\sigma_L}|\sigma_1\dots\sigma_L\rangle \in V \text{ s.t. } \dim V = d^L \tag{82}$$

Note the *abuse of notation*: while $c^{\sigma_1\dots\sigma_L} \in \mathbb{C}$ itself, also denote $c^{\sigma_1\dots\sigma_L} \in \mathbb{C}^{d^L}$ as a shorthand for $\sum_{\sigma_1\dots\sigma_L} c^{\sigma_1\dots\sigma_L}|\sigma_1\dots\sigma_L\rangle$

Reshape coefficient vector into matrix of (size) dimension $(d \times d^{L-1})$.

$$\begin{gathered} \mathbb{C}^{d^L} \xrightarrow{\text{reshape}} \text{Mat}_{\mathbb{C}}(d, d^{L-1}) \\ c^{\sigma_1\dots\sigma_L} \xmapsto{\text{reshape}} \Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} \end{gathered}$$

Then do SVD:

$$\Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} \overset{\text{SVD}}{=} \sum_{a_1} U_{\sigma_1 a_1} S_{a_1 a_1} V^\dagger_{a_1,\sigma_2\dots L} = U_{\sigma_1 a_1} S_{a_1 a_1} V^\dagger_{a_1,\sigma_2\dots\sigma_L}$$

Let's utilize commutative diagrams to summarize the reshaping and SVD operations that we've done.

$$\mathbb{C}^{d^L} = \text{Mat}_{\mathbb{C}}(1, d^L) \xrightarrow{\text{reshape}} \text{Mat}_{\mathbb{C}}(d, d^{L-1}) \xrightarrow{\text{SVD}} \text{Mat}_{\mathbb{C}}(d, r_1) \times \text{Mat}_{\mathbb{C}}(r_1, r_1) \times \text{Mat}_{\mathbb{C}}(r_1, d^{L-1})$$

$$|\Psi\rangle \equiv c^{\sigma_1\dots\sigma_L} \xmapsto{\text{reshape}} \Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} \xmapsto{\text{SVD}} \Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} \overset{\text{SVD}}{=} U_{\sigma_1 a_1} S_{a_1 a_1} V^\dagger_{a_1,\sigma_2\dots\sigma_L}$$

where I abuse notation for the SVD operation in that, SVD maps a matrix (in this case, Ψ) into 3 matrices, that obey the equality relationship when they're multiplied together (i.e. $\Psi = USV^\dagger$).

Slice U into d row vectors, i.e. for $U \in \text{Mat}_{\mathbb{C}}(d, r_1)$.

$$\begin{gathered} \text{Mat}_{\mathbb{C}}(d, r_1) \xrightarrow{\text{slice}} \text{Mat}_{\mathbb{C}}(1, r_1)^d \\ U_{\sigma_1 a_1} \mapsto \{A^{\sigma_1}\} \equiv \{A^{\sigma_1}_{1,a_1}\}_{\sigma_1} \text{ s.t. } A^{\sigma_1}_{1,a_1} = U_{\sigma_1 a_1} \text{ and } |\{A^{\sigma_1}_{1,a_1}\}| = d \end{gathered}$$

Collecting all the operations, and doing the following notation rewrite,

$$c^{\sigma_1\sigma_2\dots\sigma_L} \mapsto \Psi_{\sigma_1\sigma_2\dots\sigma_L} = \sum_{a_1} A^{\sigma_1}_{1a_1} S_{a_1 a_1} V^\dagger_{a_1,\sigma_2\dots\sigma_L} = \sum_{a_1} A^{\sigma_1}_{1a_1} c^{a_1\sigma_2\sigma_3\dots\sigma_L}$$

where

$$c^{a_1\sigma_2\sigma_3\dots\sigma_L} = S_{a_1 a_1} V^\dagger_{a_1\sigma_2\dots\sigma_L}$$

Do the same procedure again.

$$\text{Mat}_{\mathbb{C}}(r_1, d^{L-1}) \xrightarrow{\text{reshape}} \text{Mat}_{\mathbb{C}}(r_1 d, d^{L-2}) \xrightarrow{\text{SVD}} \text{Mat}_{\mathbb{C}}(r_1 d, r_2) \times \text{Mat}_{\mathbb{C}}(r_2, r_2) \times \text{Mat}_{\mathbb{C}}(r_2, d^{L-2})$$

$$c^{a_1,\sigma_2\sigma_3\dots\sigma_L} \xmapsto{\text{reshape}} \Psi_{a_1\sigma_2,(\sigma_3\dots\sigma_L)} \xmapsto{=} \Psi_{a_1\sigma_2,(\sigma_3\dots\sigma_L)} \overset{\text{SVD}}{=} U_{a_1\sigma_2,a_2} S_{a_2 a_2} V^\dagger_{a_2,\sigma_3\dots\sigma_L}$$

Then slice U into d matrices, and then matrix multiply the S and $V^\dagger$ matrices together:

$$\text{Mat}_{\mathbb{C}}(r_1 d, r_2) \times \text{Mat}_{\mathbb{C}}(r_2, r_2) \times \text{Mat}_{\mathbb{C}}(r_2, d^{L-2}) \xrightarrow{\text{slice and multiply}} \text{Mat}_{\mathbb{C}}(r_1, r_2)^d \times \text{Mat}_{\mathbb{C}}(r_2, d^{L-2})$$

$$\textstyle\sum_{a_2} U_{a_1\sigma_2,a_2} S_{a_2 a_2} V^\dagger_{a_2,\sigma_3\dots\sigma_L} \xmapsto{=} = \sum_{a_2} A^{\sigma_2}_{a_1 a_2} c^{a_2,a_3\dots\sigma_L} \text{ where } A^{\sigma_2}_{a_1 a_2} = U_{a_1\sigma_2,\sigma_3\dots\sigma_L}$$

Thus, generalize the *ith procedure*: for $i = 1 \dots L$,
Let $r_0 = 1$.

$$
\boxed{\begin{array}{ccccccc}
\mathrm{Mat}_{\mathbb{C}}(r_{i-1}, d^{L-(i-1)}) & \xrightarrow{\text{reshape}} & \mathrm{Mat}_{\mathbb{C}}(r_{i-1}d, d^{L-i}) & \xrightarrow{\text{SVD}} & \mathrm{Mat}_{\mathbb{C}}(r_{i-1}d, r_i) \times \mathrm{Mat}_{\mathbb{C}}(r_i, r_i) \times \mathrm{Mat}_{\mathbb{C}}(r_i, d^{L-i}) & \xrightarrow{\text{slice and multiply}} & \mathrm{Mat}_{\mathbb{C}}(r_{i-1}, r_i)^d \times \mathrm{Mat}_{\mathbb{C}}(r_i, d^{L-i}) \\
c^{a_{i-1}, \sigma_i \sigma_{i+1} \dots \sigma_L} & \xmapsto{\text{reshape}} & \Psi_{a_{i-1}\sigma_i, (\sigma_{i+1}\sigma_{i+2}\dots\sigma_L)} & \xmapsto{=} & U_{a_{i-1}\sigma_i, a_i} S_{a_i a_i} V^{\dagger}_{a_i, \sigma_{i+1}\dots\sigma_L} & \xmapsto{=} & A^{\sigma_i}_{a_{i-1}, a_i} c^{a_i, \sigma_{i+1}\dots\sigma_L}
\end{array}} \tag{83}
$$

Remember that $r_i \leq \min{(r_{i-1}d, d^{L-i})}$ and for $i = L$, there is no need to do a SVD, but only a reshape, and slice and multiply.
Collecting all the A matrices:

$$
\boxed{\begin{aligned}
& A^{\sigma_1}_{1,a_1} \in \mathrm{Mat}_{\mathbb{C}}(1, r_1); \qquad r_1 \leq d \\
& A^{\sigma_2}_{a_1,a_2} \in \mathrm{Mat}_{\mathbb{C}}(r_1, r_2); \qquad r_2 \leq r_1 d \\
& \vdots \\
& A^{\sigma_i}_{a_{i-1},a_i} \in \mathrm{Mat}_{\mathbb{C}}(r_{i-1}, r_i); \qquad r_i \leq \min{(r_{i-1}d, d^{L-i})} \\
& \vdots \\
& A^{\sigma_L}_{a_{L-1},a_L} \in \mathrm{Mat}_{\mathbb{C}}(r_{L-1}, 1); \qquad r_{L-1} \leq d
\end{aligned}} \tag{84}
$$

33.3.1. *Left and Right Normalization, A and B matrices, "special gauge" from normalization.* Choose orthonormal basis states $\forall\, a_l$, $\forall\, l = 1, 2, \dots L$ For

$$
\begin{aligned}
|a_l\rangle &= \sum_{a_{l-1}\sigma_l} M^{\sigma_l}_{a_{l-1}a_l} |a_{l-1}\sigma_l\rangle \\
\langle a_l'| &= \sum_{a_{l-1}'\sigma_l'} \langle a_{l-1}'\sigma_l'| (M^{\sigma_l'}_{a_{l-1}'a_l'})^*
\end{aligned}
$$

then,

$$
\begin{gathered}
\delta_{a_l' a_l} = \langle a_l' | a_l \rangle = \sum_{a_{l-1}'\sigma_l', a_{l-1}\sigma_l} M^{\sigma_l' *}_{a_{l-1}'a_l'} M^{\sigma_l}_{a_{l-1}a_l} \langle a_{l-1}'\sigma_l' | a_{l-1}\sigma_l\rangle = \sum_{a_{l-1}\sigma_l} M^{\sigma_l *}_{a_{l-1}a_l'} M^{\sigma_l}_{a_{l-1}a_l} = \\
= \sum_{\sigma_l} ((M^{\sigma_l})^\dagger M^{\sigma_l})_{a_l' a_l}
\end{gathered} \tag{85}
$$

Left normalization comes from a property of SVD in that $\forall\, U$ matrices, $U^\dagger U = 1$, and so

$$
\begin{gathered}
(U^\dagger)_{a_i' k_i} U_{k_i a_i} = \delta_{a_i' a_i} = U^*_{k_i a_i'} U_{k_i a_i} = U^*_{a_{i-1}'\sigma_i, a_i'} U_{a_{i-1}''\sigma_i, a_i} = \\
= A^{\sigma_i *}_{a_{i-1}'', a_i'} A^{\sigma_i}_{a_{i-1}'', a_i} = (A^{\sigma_i})^\dagger A^{\sigma_i} = \boxed{\sum_{\sigma_i} (A^{\sigma_i})^\dagger A^{\sigma_i} = 1}
\end{gathered} \tag{86}
$$

For right normalization, consider doing the operations of Eq. 83 "on the right":

$$
\begin{tikzcd}
\mathrm{Mat}_{\mathbb{C}}(d^L,1) \arrow[r, "\text{reshape}"] & \mathrm{Mat}_{\mathbb{C}}(d^{L-1},d) \arrow[r, "\text{SVD}"] & \mathrm{Mat}_{\mathbb{C}}(d^{L-1},r_1)\times\mathrm{Mat}_{\mathbb{C}}(r_1,r_1)\times\mathrm{Mat}_{\mathbb{C}}(r_1,d) \arrow[r, "\text{slice and multiply}"] & \mathrm{Mat}_{\mathbb{C}}(d^{L-1},r_1)\times\mathrm{Mat}_{\mathbb{C}}(r_1,1)^d \\
c^{\sigma_1\sigma_2\dots\sigma_L} \arrow[r, mapsto, "\text{reshape}"] & \Psi_{\sigma_1\dots\sigma_{L-1},\sigma_L} \arrow[r, mapsto, "="] & U_{\sigma_1\dots\sigma_{L-1}a_1}S_{a_1a_1}V^\dagger_{a_1,\sigma_L} \arrow[r, mapsto, "="] & \sum_{\sigma_L} c^{\sigma_1\dots\sigma_{L-1},a_1}B^{\sigma_L}_{a_1,1}
\end{tikzcd}
$$

$$
\begin{tikzcd}
\mathrm{Mat}_{\mathbb{C}}(d^{L-1},r_1) \arrow[r, "\text{reshape}"] & \mathrm{Mat}_{\mathbb{C}}(d^{L-2},r_1d) \arrow[r, "\text{SVD}"] & \mathrm{Mat}_{\mathbb{C}}(d^{L-2},r_2)\times\mathrm{Mat}_{\mathbb{C}}(r_2,r_2)\times\mathrm{Mat}_{\mathbb{C}}(r_2,r_1d) \arrow[r, "\text{slice and multiply}"] & \mathrm{Mat}_{\mathbb{C}}(d^{L-2},r_2)\times\mathrm{Mat}_{\mathbb{C}}(r_2,r_1)^d \\
c^{\sigma_1\dots\sigma_{L-1}a_1} \arrow[r, mapsto, "\text{reshape}"] & \Psi_{\sigma_1\dots\sigma_{L-2},\sigma_{L-1}a_1} \arrow[r, mapsto, "="] & U_{\sigma_1\dots\sigma_{L-2},a_2}S_{a_2a_2}V^\dagger_{a_2,\sigma_{L-1}a_1} \arrow[r, mapsto, "="] & \sum_{\sigma_{L-1}} c^{\sigma_1\dots\sigma_{L-2},a_2}B^{\sigma_{L-1}}_{a_2,a_1}
\end{tikzcd}
$$

$$\vdots$$

$$
\boxed{
\begin{tikzcd}
\mathrm{Mat}_{\mathbb{C}}(d^{L-(i-1)},r_{i-1}) \arrow[r, "\text{reshape}"] & \mathrm{Mat}_{\mathbb{C}}(d^{L-i},r_{i-1}d) \arrow[r, "\text{SVD}"] & \mathrm{Mat}_{\mathbb{C}}(d^{L-i},r_i)\times\mathrm{Mat}_{\mathbb{C}}(r_i,r_i)\times\mathrm{Mat}_{\mathbb{C}}(r_i,r_{i-1}d) \arrow[r, "\text{slice and multiply}"] & \mathrm{Mat}_{\mathbb{C}}(d^{L-i},r_i)\times\mathrm{Mat}_{\mathbb{C}}(r_i,r_{i-1})^d \\
c^{\sigma_1\dots\sigma_{L-(i-1)}a_{i-1}} \arrow[r, mapsto, "\text{reshape}"] & \Psi_{\sigma_1\dots\sigma_{L-i},\sigma_{L-(i-1)}a_{i-1}} \arrow[r, mapsto, "="] & U_{\sigma_1\dots\sigma_{L-i},a_i}S_{a_ia_i}V^\dagger_{a_i,\sigma_{L-(i-1)}a_{i-1}} \arrow[r, mapsto, "="] & \sum_{\sigma_{L-(i-1)}} c^{\sigma_1\dots\sigma_{L-i},a_i}B^{\sigma_{L-(i-1)}}_{a_i,a_{i-1}}
\end{tikzcd}
} \tag{87}
$$

Remember that $r_i \leq \min(d^{L-i}, r_{i-1}d)$ and for $i=L$, just do reshape and slice and multiply operations.

Then, finally, the **right normalization** is derived and is such:

$$
\begin{gathered}
V^\dagger V = 1 \Longrightarrow \\
(V^\dagger V)_{a_ia_i'} = \delta_{a_ia_i'} = V^\dagger_{a_i,\sigma_{L-(i-1)}a_{i-1}} V_{\sigma_{L-(i-1)}a_{i-1},a_i'} = B^{\sigma_{L-(i-1)}}_{a_i,a_{i-1}}(V^\dagger)^\dagger_{\sigma_{L-(i-1)}a_{i-1},a_i'} = \\
= B^{\sigma_{L-(i-1)}}_{a_ia_{i-1}}(V^\dagger)^*_{a_i',\sigma_{L-(i-1)},a_{i-1}} = B^{\sigma_{L-(i-1)}}_{a_i,a_{i-1}}B^{\sigma_{L-(i-1)}}_{a_i',a_{i-1}} = B^{\sigma_{L-(i-1)}}_{a_ia_{i-1}}(B^\dagger)^{\sigma_{L-(i-1)}}_{a_{i-1}a_i'} \qquad \forall i = 1\dots L \\
\Longrightarrow \sum_{\sigma_{L-(i-1)}} B^{\sigma_{L-(i-1)}}(B^\dagger)^{\sigma_{L-(i-1)}} = 1
\end{gathered} \tag{88}
$$

cf. Sec. 4, Matrix Product States (MPS) of Schollwöck [19].

Necessarily, given matrix $M \in \mathrm{Mat}_{\mathbb{K}}(M,N)$ (notation in Bridgeman and Chubb (2017) [17] and CUDA Toolkit Documentation; I will follow the notation in Schollwöck [19] since his A,B denote specific physical meaning).

For

$$U \in \mathrm{Mat}_{\mathbb{K}}(N_A, \min(N_A,N_B)) \text{ s.t. } UU^\dagger = 1$$

$$S \in \mathrm{Mat}_{\mathbb{K}}(\min(N_A,N_B), \min(N_A,N_B))$$

s.t. S diagonal with nonnegative $S_{aa} = s_a$, i.e. $S_{ij} = \delta_{ij}s_i$ s.t. $s_i \geq 0 \quad \forall i = 1,2,\dots\min(N_A,N_B)$.

$r \equiv$ (Schmidt) rank of $M :=$ number of nonzero singular values.

Assume $s_1 \geq s_2 \geq \dots \geq s_r \geq 0$.

$V^\dagger \in \mathrm{Mat}_{\mathbb{K}}(\min(N_A,N_B),N_B)$ s.t. $V^\dagger V = 1$.

$$
\begin{tikzcd}
\mathrm{Mat}_{\mathbb{K}}(N_A,N_B) \arrow[r, "\text{SVD}"] & U_{\mathbb{K}}(N_A,\min(N_A,N_B))\times\mathrm{diag}_{\mathbb{K}}(\min(N_A,N_B))\times U_{\mathbb{K}}(\min(N_A,N_B),N_B) \\
M \arrow[r, mapsto, "\text{SVD}"] & USV^\dagger
\end{tikzcd}
$$

Optimal approximation of M (rank r by matrix M' (rank $r' < r$) property.

In Frobenius norm $\|M\|_F^2 := \sum_{i,j}|M_{ij}|^2$, induced by inner product $\langle M|N\rangle = \mathrm{tr}M^\dagger N$. Indeed,

$$\mathrm{tr}M^\dagger N = (M^\dagger)_{ik}N_{ki} = \overline{M}_{ki}N_{ki}$$

and so for

$$M' = US'V^\dagger, \qquad S' = \mathrm{diag}(s_1, s_2\dots s_{r'}, 0\dots) \tag{89}$$

cf. Eq. (19) of Schollwöck [19], i.e. 1 sets all but 1st r' singualr values to 0.

Use singular value decomposition (SVD) to derive Schmidt decomposition of general quantum state.

$\forall$ pure state $|\psi\rangle$ on AB,

$$|\psi\rangle = \sum_{i,j} \Psi_{ij} |i\rangle_A |j\rangle_B$$

where $\{|i\rangle_A\}, \{|j\rangle_B\}$ orthonormal bases of A, B ((complex) Hilbert spaces), with dim. N_A, N_B, respectively.

Let $\Psi_{i,j} \in \text{Mat}_{\mathbb{K}}(N_A, N_B)$.

Then **reduced density operators** $\widehat{\rho}_A, \widehat{\rho}_B$ are such that

$$\begin{aligned} \widehat{\rho}_A &= \text{tr}_B |\psi\rangle\langle\psi| \\ \widehat{\rho}_B &= \text{tr}_A |\psi\rangle\langle\psi| \end{aligned}$$

In matrix form,

$$\begin{aligned} \rho_A &= \Psi\Psi^\dagger \\ \rho_B &= \Psi^\dagger\Psi \end{aligned}$$

Indeed,

$$\begin{aligned} (\rho_A)_{ij} &= \Psi_{ik}\overline{\Psi}_{jk} \\ (\rho_B)_{ij} &= \overline{\Psi}_{ki}\Psi_{kj} \\ |\psi\rangle\langle\psi| &= \sum_{i,j} \Psi_{ij}|i\rangle_A|j\rangle_B \sum_{l,m} \overline{\Psi}_{lm}\langle l|_A\langle m|_B \\ \text{tr}_B|\psi\rangle\langle\psi| &= \sum_{i,j} \Psi_{ik}\overline{\Psi}_{jk}|i\rangle_A\rangle j|_A \end{aligned}$$

In matrix form,

$$\begin{aligned} \rho_A &= \Psi\Psi^\dagger \\ \rho_B &= \Psi^\dagger\Psi \end{aligned}$$

Carry out SVD on Ψ in Eq. (20) of Schollwöck [19],

$$|\psi\rangle = \sum_{i,j} \Psi_{ij}|i\rangle_A|j\rangle_B$$

$$|\psi\rangle = \sum_{ij} \Psi_{ij}|i\rangle_A|j\rangle_B = \sum_{ij}\sum_{a=1}^{\min(N_A,N_B)} U_{ia}S_{aa}\overline{V}_{ja}|i\rangle_A|j\rangle_B = \sum_{a=1}^{\min(N_A,N_B)} \sum_i U_{ia}|i\rangle_A s_a \sum_j \overline{V}_{ja}|j\rangle_B = \sum_{a=1}^{\min(N_A,N_B)} s_a|a\rangle_A|a\rangle_B$$

Due to orthogonality of $U, V^\dagger$, $\{|a\rangle_A\}, \{|a\rangle_B\}$ orthonormal, and can be extended to be orthonormal bases of A, B.

If we restrict the sum to run only over the $r \leq \min(N_A, N_B)$ positive nonzero singular values (i.e., for $\sum_{a=1}^{\min(N_A,N_B)}$, $_a > 0$ $\forall a \leq r$, and so

$$|\psi\rangle = \sum_{a=1}^r s_a|a\rangle_A|a\rangle_B$$

$r = 1$ (classical) product states. $|\psi\rangle = s_1|1\rangle_A|1\rangle_B$.
$r > 1$ entangled (quantum) states.

Schmidt decomposition on reduced density operators for A and B:

$$\begin{aligned} \widehat{\rho}_A &= \sum_{a=1}^r s_a^2|a\rangle_A\langle a|_A \\ \widehat{\rho}_B &= \sum_{a=1}^r s_a^2|a\rangle_B\langle a|_B \end{aligned}$$

Respective eigenvectors are left and right singular vectors.

Von Neumann entropy can be read off:

$$S_{A|B}(|\psi\rangle) = -\text{tr}\widehat{\rho}_A \log_2 \widehat{\rho}_A = -\sum_{a=1}^r s_a^2 \log_2 s_a^2$$

In view of large size of Hilbert spaces, approximate $|\psi\rangle$ by some $|\widetilde{\psi}\rangle$ spanned over state spaces A, B that have dims. r' only.

Since 2-norm of $|\psi\rangle$,

$$\||\psi\rangle\|_2^2 = \sum_{ij} |\Psi_{ij}|^2 = \|\Psi\|_F^2$$

since

$$\||\psi\rangle\|_2^2 = \sum_{a=1}^r s_a^2 = \sum_{ij} |\Psi_{ij}|^2$$

iff $\{|i\rangle\}, \{|j\rangle\}$ orthonormal. Optimal approx. of 2-norm given by optimal approx. of Ψ by $\overline{\Psi}$ in Frobenius norm, where $\overline{\Psi}$ is matrix of rank r'.

$\overline{\Psi} = US'V^\dagger$, $S' = \text{diag}(s_1, \dots s_{r'}, 0\dots)$ from above.

$\Longrightarrow$ Schmidt decomposition of approximate state

$$|\overline{\Psi}\rangle = \sum_{a=1}^{r'} s_a|a\rangle_A|a\rangle_B \tag{90}$$

cf. Eq. (27) of Schollwöck [19], where s_a must be rescaled if normalization desired.

33.4. QR decomposition. cf. 4.1.2. of Schollwöck [19].

If actual value of singular values not used explicitly, then use *QR decomposition*.

QR decomposition: $\forall M \in \text{Mat}_{\mathbb{K}}(N_A, N_B)$,

$$M = QR,\ Q \in U_{\mathbb{K}}(N_A), \text{ i.e. } Q^\dagger Q = 1 = QQ^\dagger,\ R \in \text{Mat}_{\mathbb{K}}(N_A, N_B) \text{ s.t. upper triangular, i.e. } R_{ij} = 0 \text{ if } i > j \tag{91}$$

thin QR decomposition: assume $N_A > N_B$. Then bottom $N_A - N_B$ rows of R are 0, so

$$\begin{aligned} M = Q\begin{bmatrix} R_1 \\ 0 \end{bmatrix} &= \begin{bmatrix} Q_1 & Q_2 \end{bmatrix}\begin{bmatrix} R_1 \\ 0 \end{bmatrix} = Q_1R_1 \\ Q_1 &\in \text{Mat}_{\mathbb{K}}(N_A, N_B) \\ R_1 &\in \text{Mat}_{\mathbb{K}}(N_B, N_B) \end{aligned}$$

While $Q_1^\dagger Q_1 = 1$ in general $Q_1Q_1^\dagger \neq 1$

34. Matrix Product States (MPS)

cf. Section 4.13 Decomposition of arbitrary quantum states into MPS of Schollwöck [19].

Consider lattice of L sites, d-dim. local state spaces $\{\sigma_i\}_{i=1,\dots L}$.

Most general pure quantum state on lattice (assume normalized)

$$|\psi\rangle = \sum_{\sigma_1\dots\sigma_L} c_{\sigma_1\dots\sigma_L}|\sigma_1\dots\sigma_L\rangle \tag{92}$$

cf. Eq. (30) of Schollwöck [19],

34.1. **Left-canonical matrix product state.** cf. Schollwöck [19],

Consider the process of refactoring or "flattening", which I claim to be a functor *flatten*:

$$|\psi\rangle \in \mathcal{H} \text{ s.t. } \dim \mathcal{H} = d^L \mapsto \Psi \in \mathrm{Mat}_{\mathbb{K}}(d, d^{L-1})$$

$$\Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} = c_{\sigma_1\dots\sigma_L}$$

$$\xrightarrow{\text{SVD}} c_{\sigma_1\dots\sigma_L} = \Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} = \sum_a^{r_1} U_{\sigma_1,a_1} S_{a_1,a_1} (V^\dagger)_{a_1,(\sigma_2\dots\sigma_L)} \equiv \sum_{a_1}^{r_1} U_{\sigma_1,a_1} c_{a_1,\sigma_2\dots\sigma_L} \tag{93}$$

i.e.

$$(\mathbb{K}^d)^L \to \mathrm{Mat}_{\mathbb{K}}(1,r) \times \mathrm{Mat}_{\mathbb{K}}(r_1 d, d^{L-2})$$
$$c_{\sigma_1\dots\sigma_L} \mapsto A^{\sigma_1}_{a_1}, \Psi_{(a_1\sigma_2),(\sigma_3\dots\sigma_L)}$$

s.t.

$$c_{\sigma_1\dots\sigma_L} = \sum_{a_1}^{r_1} A^{\sigma_1}_{a_1} \Psi_{(a_1\sigma_2),(\sigma_3\dots\sigma_L)}$$

where rank $r_1 \leq d$.

$$U \in \mathrm{Mat}_{\mathbb{K}}(d, \min(d,r)) = \mathrm{Mat}_{\mathbb{K}}(d,r)$$

Consider d row vectors A^{σ_1}, $A^{\sigma_1}_{a_1} = U_{\sigma_1,a_1}$.

$$c_{a_1\sigma_2\dots\sigma_L} = \sum_{a_1}^{r_1} A^{\sigma_1}_{a_1} \Psi_{(a_1,\sigma_2),(\sigma_3\dots\sigma_L)} \text{ with}$$

$$\Psi_{(a_1\sigma_2),(\sigma_3\dots\sigma_L)} \in \mathrm{Mat}_{\mathbb{K}}(r_1 d, d^{L-2})$$

So from Eq. (34) of Schollwöck [19],

$$c_{\sigma_1\dots\sigma_L} = \sum_{a_1}^{r_1}\sum_{a_2}^{r_2} A^{\sigma_1}_{a_1} U_{(a_1\sigma_2),a_2} S_{a_2,a_2} (V^\dagger)_{a_2,(\sigma_3\dots\sigma_L)} = \sum_{a_1}^{r_1}\sum_{a_2}^{r_2} A^{\sigma_1}_{a_1} A^{\sigma_2}_{a_1,a_2} \Psi_{(a_2\sigma_3),(\sigma_4\dots\sigma_L)} \tag{94}$$

So for

$$U \in \mathrm{Mat}_{\mathbb{K}}(d, r_1 \times r_2) \mapsto \{A^{\sigma_2}\}_{\sigma_2}, \qquad |\{A^{\sigma_2}\}_{\sigma_2}| = d, \qquad A^{\sigma_2} \in \mathrm{Mat}_{\mathbb{K}}(r_1, r_2)$$

$A^{\sigma_2}_{a_1,a_2} = U_{(a_1,\sigma_2),a_2}$ and multiplied S and $V^\dagger$,

$$SV^\dagger \mapsto \Psi \in \mathrm{Mat}_{\mathbb{K}}(r_2 d, d^{L-3}); \qquad r_2 \leq r_1 d \leq d^2$$

and so continuing the application of SVD and refactoring (what I call applying the *flatten* functor)

$$\xrightarrow{\text{SVD}} c_{\sigma_1\dots\sigma_L} = \sum_{a_1\dots a_{L-1}} A^{\sigma_1}_{a_1} A^{\sigma_2}_{a_1 a_2} \dots A^{\sigma_{L-1}}_{a_{L-2},a_{L-1}} A^{\sigma_L}_{a_L-1} \equiv A^{\sigma_1}A^{\sigma_2}\dots A^{\sigma_{L-1}}A^{\sigma_L}$$

34.1.1. *Matrix Product State (definition).*

Definition 79 (Matrix Product State)**.**

$$|\psi\rangle = \sum_{\sigma_1\dots\sigma_L} A^{\sigma_1}A^{\sigma_2}\dots A^{\sigma_{L-1}}A^{\sigma_L}|\sigma_1\dots\sigma_L\rangle \tag{95}$$

Maximally, the dims. are

$$(1\times d),(d\times d^2)\dots(d^{L/2-1}\times d^{L/2}),(d^{L/2}\times d^{L/2-1})\dots(d^2\times d),(d\times 1)$$

Since $\forall$ SVD, $U^\dagger U = 1$,

$$\delta_{a_l,a_l'} = \sum_{a_{l-1}a_l} (U^\dagger)_{a_l,(a_{l-1}\sigma_l)} U_{(a_{l-1}\sigma_l),a_l'} = \sum_{a_{l-1}\sigma_l} (A^{\sigma_l})^\dagger_{a_l,a_{l-1}} A^{\sigma_l}_{a_{l-1},a_l'} = \sum_{\sigma_l} ((A^{\sigma_2})^\dagger A^{\sigma_l})_{a_l,a_l'}$$

or

$$\sum_{\sigma_l} (A^{\sigma_l})^\dagger A^{\sigma_l} = 1 \tag{96}$$

cf. Eq. (38) of Schollwöck [19],

If for $\{A^{\sigma_l}\}_{\sigma_l}$, $\sum_{\sigma_l}(A^{\sigma_l})^\dagger A = 1$, $\{A^{\sigma_l}\}_{\sigma_l}$ are **left-normalized**; matrix product states that consist of only left-normalized matrices are **left-canonical**.

View Density Matrix Renormalization Group (DMRG) decomposition of universe into blocks A and B, split lattice into parts A,B, where A compries sites 1 through l and B sites $l+1$ through L.

$$|a_l\rangle_A = \sum_{\sigma_1\dots\sigma_l} (A^{\sigma_1}A^{\sigma_2}\dots A^{\sigma_l})_{a_l,1}|\sigma_1\dots\sigma_l\rangle$$
$$|a_l\rangle_B = \sum_{\sigma_{l+1}\dots\sigma_L} (A^{\sigma_{l+1}}A^{\sigma_{l+2}}\dots A^{\sigma_L})_{a_l,1}|\sigma_{l+1}\dots\sigma_L\rangle$$

s.t. matrix product state (MPS) is

$$|\psi\rangle = \sum_{a_l} |a_l\rangle_A |a_l\rangle_B$$

34.1.2. *Summarize this procedure of constructing, from a pure state, the matrix product state (version) by successive application Singular Value Decomposition (SVD) from the Category Theory point of view.* Consider all applications of SVD to get to a matrix

$$(\mathbb{K}^d)^L \xrightarrow{\text{SVD}} (\mathrm{Mat}_{\mathbb{K}}(1,r_1))^d \times (\mathrm{Mat}_{\mathbb{K}}(r_1,r_2))^d \times \dots \times (\mathrm{Mat}_{\mathbb{K}}(r_{L-2},r_{L-1}))^d \times (\mathrm{Mat}_{\mathbb{K}}(r_{L-1},1))^d$$

$$c_{\sigma_1\dots\sigma_L} \xmapsto{\text{SVD}} c_{\sigma_1\dots\sigma_L} = \textstyle\sum_{a_1\dots a_{L-1}} A^{\sigma_1}_{a_1}A^{\sigma_2}_{a_1a_2}\dots A^{\sigma_{L-1}}_{a_{L-2},a_{L-1}}A^{\sigma_L}_{a_{L-1}}$$

product state (MPS):

and remember the maximal values that the r_i's can take:

$$\begin{array}{lll} r_1 \leq d & r_{L/2} \leq d^{L/2} & r_{L-2} \leq d^2 \\ r_2 \leq d^2 & r_{L/2+1} \leq d^{L/2-1} & r_{L-1} \leq d \end{array}$$

Let us explicitly note the functors (that were applied) flatten (and its inverse), and the application of SVD, explicitly:

$$\begin{array}{c} (\mathbb{K}^d)^L \xrightarrow{\text{flatten}^{-1}} \text{Mat}_{\mathbb{K}}(d,d^{L-1}) \xrightarrow{\text{SVD}} U_{\mathbb{K}}(d,r_1)\times\text{diag}_{\mathbb{K}}(r_1)\times U_{\mathbb{K}}(r_1,d^{L-1}) \xrightarrow{\cong} (\text{Mat}_{\mathbb{K}}(1,r_1))^d\times\text{Mat}_{\mathbb{K}}(r_1d,d^{L-2}) \xrightarrow{\text{flatten}} (\text{Mat}_{\mathbb{K}}(1,r_1))^d\times(\mathbb{K}^{r_1})\times(\mathbb{K}^d)^{L-1} \\ \\ c_{\sigma_1\dots\sigma_L} \xmapsto{\text{flatten}^{-1}} c_{\sigma_1\dots\sigma_L} = \Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} \xmapsto{\text{SVD}} \Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} = \sum_{a_1}^{r_1} U_{\sigma_1a_1}S_{a_1,a_1}(V^\dagger)_{a_1,(\sigma_2\dots\sigma_L)} \xmapsto{\cong} c_{a_1\sigma_2\dots\sigma_L} = \sum_{a_1}^{r_1} A^{\sigma_1}_{a_1}\Psi_{(a_1,a_2),(\sigma_3\dots\sigma_L)} \xmapsto{\text{flatten}} c_{a_1\sigma_2\dots\sigma_L} = \sum_{a_1}^{r_1} A^{\sigma_1}_{a_1}c_{a_1\sigma_2\dots\sigma_L} \end{array}$$

with $\cong$ in this case denoting an isomorphism (clearly).

In considering some kind of recursive algorithm, so to repeat some series of steps until a matrix product state is obtained, consider this:

$$\begin{array}{c} (\mathbb{K}^d)^L \longrightarrow (\text{Mat}_{\mathbb{K}}(1,r_1))^d\times\mathbb{K}^{r_1}\times(\mathbb{K}^d)^{L-1} \\ \\ c_{\sigma_1\dots\sigma_L} \longmapsto c_{\sigma_1\dots\sigma_L} = \sum_{a_1}^{r_1} A^{\sigma_1}_{a_1}c_{a_1\sigma_2\dots\sigma_L} \end{array}$$

So in summary, to obtain matrix product states, starting from a matrix,

$$\boxed{\begin{array}{c} \text{Mat}_{\mathbb{K}}(d,d^{L-1}) \longrightarrow (\text{Mat}_{\mathbb{K}}(1,r_1))^d\times\text{Mat}_{\mathbb{K}}(r_1d,d^{L-2}) \longrightarrow \dots \longrightarrow (\text{Mat}_{\mathbb{K}}(1,r_1))^d\times(\text{Mat}_{\mathbb{K}}(r_1,r_2))^d\times\dots\times(\text{Mat}_{\mathbb{K}}(r_{n-1},r_n))^d\times(\text{Mat}_{\mathbb{K}}(r_nd,d^{L-(n+1)}))^d \\ \\ \Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} \longmapsto \sum_{a_1}^{r_1} A^{\sigma_1}_{a_1}\Psi_{(a_1,\sigma_2),(\sigma_3\dots\sigma_L)} \longmapsto \dots \longmapsto \sum_{a_1,a_2,\dots a_n}^{r_1,r_2,\dots r_n} A^{\sigma_1}_{a_1}A^{\sigma_2}_{a_1a_2}\dots A^{\sigma_n}_{a_{n-1}a_n}\Psi_{(a_n\sigma_{n+1}),(\sigma_{n+2}\dots\sigma_L)} \end{array}} \tag{97}$$

34.2. **Right-canonical matrix product state.** cf. Schollwöck [19],

We can start from right in order to obtain

$$c_{\sigma_1\dots\sigma_L} = \Psi_{(\sigma_1\dots\sigma_{L-1}),\sigma_L} = \sum_{a_{L-1}} U_{(\sigma_1\dots\sigma_{L-1}),a_{L-1}}S_{a_{L-1},a_{L-1}}(V^\dagger)_{a_{L-1},\sigma_L} = \sum_{a_{L-1}}\Psi_{(\sigma_1\dots\sigma_{L-2}),(\sigma_{L-1}a_{L-1})}B^{\sigma_L}_{a_{L-1}} =$$
$$= \sum_{a_{L-1},a_{L-2}} U_{(\sigma_1\dots\sigma_{L-2}),a_{L-2}}S_{a_{L-2},a_{L-2}}(V^\dagger)_{a_{L-2},(\sigma_{L-1}a_{L-1})}B^{\sigma_L}_{a_{L-1}} = \sum_{a_{L-2},a_{L-1}}\Psi_{(\sigma_1\dots\sigma_{L-3}),(\sigma_{L-2}a_{L-2})}B^{\sigma_{L-1}}_{a_{L-2},a_{L-1}}B^{\sigma_L}_{a_{L-1}} = \dots$$

or consider

$$\begin{array}{c} (\mathbb{K}^d)^L \xrightarrow{\text{flatten}^{-1}} \text{Mat}_{\mathbb{K}}(d^{L-1},d) \xrightarrow{\text{SVD}} U_{\mathbb{K}}(d^{L-1},r_{L-1})\times\text{diag}_{\mathbb{K}}(r_{L-1})\times U_{\mathbb{K}}(r_{L-1},d) \xrightarrow{\cong} \text{Mat}_{\mathbb{K}}(d^{L-2},dr_{L-1})\times(\text{Mat}_{\mathbb{K}}(r_{L-1},1))^d \xrightarrow{\text{SVD}} \\ \\ c_{\sigma_1\dots\sigma_L} \xmapsto{\text{flatten}^{-1}} c_{\sigma_1\dots\sigma_L} = \Psi_{(\sigma_1\dots\sigma_{L-1}),\sigma_L} \xmapsto{\text{SVD}} c_{\sigma_1\dots\sigma_L} = \sum_{a_{L-1}}^{r_{L-1}} U_{(\sigma_1\dots\sigma_{L-1}),a_{L-1}}S_{a_{L-1},a_{L-1}}(V^\dagger)_{a_{L-1},\sigma_L} \xmapsto{\cong} \begin{gathered} U_{(\sigma_1\dots\sigma_{L-1}),a_{L-1}}S_{a_{L-1},a_{L-1}} = \Psi_{(\sigma_1\dots\sigma_{L-2}),(\sigma_{L-1}a_{L-1})} \\ (V^\dagger)_{a_{L-1},\sigma_L} = B^{\sigma_L}_{a_{L-1}} \\ c_{\sigma_1\dots\sigma_L} = \sum_{a_{L-1}}\Psi_{(\sigma_1\dots\sigma_{L-2}),(\sigma_{L-1},a_{L-1})}B^{\sigma_L}_{a_{L-1}} \end{gathered} \xmapsto{\text{SVD}} \end{array}$$

$$\begin{array}{c} \xrightarrow{\text{SVD}} U_{\mathbb{K}}(d^{L-2},r_{L-2})\times\text{diag}_{\mathbb{K}}(r_{L-2})\times U_{\mathbb{K}}(r_{L-2},dr_{L-1})\times(\text{Mat}_{\mathbb{K}}(r_{L-1},1))^d \xrightarrow{\cong} \text{Mat}_{\mathbb{K}}(d^{L-3},dr_{L-2})\times(\text{Mat}_{\mathbb{K}}(r_{L-2},r_{L-1}))^d\times(\text{Mat}_{\mathbb{K}}(r_{L-1},1))^d \\ \\ \xmapsto{\text{SVD}} c_{\sigma_1\dots\sigma_L} = \sum_{a_{L-1},a_{L-2}} U_{(\sigma_1\dots\sigma_{L-2}),a_{L-2}}S_{a_{L-2},a_{L-2}}(V^\dagger)_{a_{L-2},(\sigma_{L-1}a_{L-1})}B^{\sigma_L}_{a_{L-1}} \xmapsto{\cong} \begin{gathered} U_{(\sigma_1\dots\sigma_{L-2}),a_{L-2}}S_{a_{L-2},a_{L-2}} = \Psi_{(\sigma_1\dots\sigma_{L-3}),(\sigma_{L-2}a_{L-2})} \\ (V^\dagger)_{a_{L-2},(\sigma_{L-1}a_{L-1})} = B^{\sigma_{L-1}}_{a_{L-2}a_{L-1}} \\ c_{\sigma_1\dots\sigma_L} = \sum_{a_{L-1},a_{L-2}}\Psi_{(\sigma_1\dots\sigma_{L-3}),(\sigma_{L-2},a_{L-2})}B^{\sigma_{L-1}}_{a_{L-2},a_{L-1}}B^{\sigma_L}_{a_{L-1}} \end{gathered} \end{array}$$

with $\cong$ in this case denoting an isomorphism (clearly).

And so we can explicitly state the recursion step, for the purpose of writing numerical implementations/algorithms: $\forall\, l = 1, 2 \dots L$,

$$\begin{aligned} \mathrm{Mat}_{\mathbb{K}}(d^{L-l}, dr_{L-(l-1)}) &\longrightarrow \mathrm{Mat}_{\mathbb{K}}(d^{L-(l+1)}, dr_{L-l}) \times (\mathrm{Mat}_{\mathbb{K}}(r_{L-l}, r_{L-(l-1)}))^d \\ \Psi_{(\sigma_1 \dots \sigma_{L-l}),(\sigma_{L-(l-1)}a_{L-(l-1)})} &\longmapsto \Psi_{(\sigma_1 \dots \sigma_{L-l}),(\sigma_{L-(l-1)}a_{L-(l-1)})} = \textstyle\sum_{a_{L-l}} \Psi_{(\sigma_1 \dots \sigma_{L-(l+1)}),(\sigma_{L-l}a_{L-l})} B^{\sigma_{L-(l-1)}}_{a_{L-l},a_{L-(l-1)}} \end{aligned}$$

and we finally obtained, after successive applications SVD, the matrix product state:

$$\begin{aligned} (\mathbb{K}^d)^L &\longrightarrow \mathrm{Mat}_{\mathbb{K}}(d^{L-1}, d) \longrightarrow (\mathrm{Mat}_{\mathbb{K}}(1, r_1))^d \times (\mathrm{Mat}_{\mathbb{K}}(r_1, r_2))^d \times \dots \times (\mathrm{Mat}_{\mathbb{K}}(r_{L-2}, r_{L-1}))^d \times (\mathrm{Mat}_{\mathbb{K}}(r_{L-1}, 1))^d \\ c_{\sigma_1 \dots \sigma_L} &\longmapsto \Psi_{(\sigma_1 \dots \sigma_{L-l}),\sigma_L} \longmapsto c_{\sigma_1 \dots \sigma_L} = \textstyle\sum_{a_1 \dots a_{L-1}} B^{\sigma_1}_{a_1} B^{\sigma_2}_{a_1 a_2} \dots B^{\sigma_{L-1}}_{a_{L-2}a_{L-1}} B^{\sigma_L}_{a_{L-1}} \end{aligned}$$

Since

$$V^\dagger V = 1 \tag{98}$$

, then

$$\delta_{a_l a'_l} = \sum_{\sigma_m a_m} (V^\dagger)_{a_l(\sigma_m a_m)} V_{(\sigma_m a_m)a'_l} = \sum_{\sigma_m a_m} B^{\sigma_m}_{a_l a_m} \overline{B}^{\sigma_m}_{a'_l a_m} \Longrightarrow \sum_{\sigma_m} \boxed{B^{\sigma_m}(B^{\sigma_m})^\dagger = 1} \tag{99}$$

The B-matrices that obey this condition are referred to as **right-normalized** matrices. A matrix product state (MPS) entirely consisting of a product of these right-normalized matrices is called **right-canonical**.

34.3. **Matrix Product Operators (MPO).** The form of a general operator, $\widehat{O}$ is the following:

$$\widehat{O} = \sum_{\{\sigma\}} \sum_{\{\sigma'\}} c^{\sigma_1 \dots \sigma_L, \sigma'_1 \dots \sigma'_L} |\sigma_1 \dots \sigma_L\rangle\langle\sigma'_1 \dots \sigma'_L| \in \mathcal{H} \otimes \mathcal{H}^* \tag{100}$$

with $\dim\mathcal{H} = \dim\mathcal{H}^* = d^L$.

For MPO, do the same decomposition as done in Eq. 83 or in **??**, but with the double index $\sigma_i\sigma'_i$ taking the role of index σ_i in MPS (i.e. do this substitution and the decomposition will proceed *exactly* as before).

$$\begin{tikzcd}
\mathrm{Mat}_{\mathbb{C}}(d^L, d^L) \arrow[d, "\text{reorder}"] \\
\mathrm{Mat}_{\mathbb{C}}(1,(d^2)^L) \arrow[r, "\text{reshape}"] & \mathrm{Mat}_{\mathbb{C}}(d^2,(d^2)^{L-1}) \arrow[r, "\text{SVD}"] & \mathrm{Mat}_{\mathbb{C}}(d^2,r_i)\times \mathrm{Mat}_{\mathbb{C}}(r_i,r_i)\times \mathrm{Mat}_{\mathbb{C}}(r_i,(d^2)^{L-1}) \arrow[r, "\text{slice and multiply}"] & \mathrm{Mat}_{\mathbb{C}}(1,r_i)^d\times \mathrm{Mat}_{\mathbb{C}}(r_i,(d^2)^{L-1})
\end{tikzcd}$$

$$\begin{tikzcd}
c^{\sigma_1\dots\sigma_L,\sigma_1'\dots\sigma_L'} \arrow[d, mapsto, "\text{reorder}"] \\
c^{\sigma_1\sigma_1'\sigma_2\sigma_2'\dots\sigma_L\sigma_L'} \arrow[r, mapsto, "\text{reshape}"] & \Psi_{\sigma_1\sigma_1',(\sigma_2\sigma_2',\sigma_3\sigma_3'\dots\sigma_L\sigma_L')} \arrow[r, mapsto, "="] & U_{\sigma_1\sigma_1',a_1}S_{a_1a_1}V^\dagger_{a_1,(\sigma_2\sigma_2'\dots\sigma_L\sigma_L'} \arrow[r, mapsto, "="] & \sum_{\sigma_1\sigma_1'}A^{\sigma_1\sigma_1'}_{1,a_1}c^{a_1,\sigma_2\sigma_2'\dots\sigma_L\sigma_L'}
\end{tikzcd}$$

$$\boxed{\begin{tikzcd}
\mathrm{Mat}_{\mathbb{C}}(r_{i-1},(d^2)^{L-(i-1)}) \arrow[r, "\text{reshape}"] & \mathrm{Mat}_{\mathbb{C}}(r_{i-1}d^2,(d^2)^{L-i}) \arrow[r, "\text{SVD}"] & \mathrm{Mat}_{\mathbb{C}}(r_{i-1}d^2,r_i)\times \mathrm{Mat}_{\mathbb{C}}(r_i,r_i)\times \mathrm{Mat}_{\mathbb{C}}(r_i,(d^2)^{L-i}) \arrow[r, "\text{slice and multiply}"] & \mathrm{Mat}_{\mathbb{C}}(r_{i-1},r_i)^{d^2}\times \mathrm{Mat}_{\mathbb{C}}(r_i,(d^2)^{L-i}) \\
c^{a_{i-1},\sigma_i\sigma_i'\sigma_{i+1}\sigma_{i+1}'\dots\sigma_L\sigma_L'} \arrow[r, mapsto, "\text{reshape}"] & \Psi_{a_{i-1}\sigma_i\sigma_i',(\sigma_{i+1}\sigma_{i+1}'\sigma_{i+2}\sigma_{i+2}'\dots\sigma_L\sigma_L')} \arrow[r, mapsto, "="] & U_{a_{i-1}\sigma_i\sigma_i',a_i}S_{a_ia_i}V^\dagger_{a_i,\sigma_{i+1}\sigma_{i+1}'\dots\sigma_L\sigma_L'} \arrow[r, mapsto, "="] & \sum_{\sigma_i\sigma_i'}^{max}A^{\sigma_i\sigma_i'}_{a_{i-1},a_i}c^{a_i,\sigma_{i+1}\sigma_{i+1}'\dots\sigma_L\sigma_L'}
\end{tikzcd}} \tag{101}$$

34.3.1. *Numerical implementation; both in BLAS and cuBLAS.* As stated in the CUDA Toolkit Documentation v8.0 for cuSOLVER, under section 5.3.6. `cusolverDn<t>gesvd()` and Remark 1, `gesvd` "only supports" `m>=n`, for matrix you want to decompose $A \in \mathrm{Mat}_{\mathbb{K}}(m,n)$. So number of rows must be greater than or equal to number of columns. And so we can only consider right-normalized matrices in a practical implementation.

I suspect it's the same in BLAS.

Consider the very first step, $l=1$, in a procedure to calculate the matrix product state.

$$\mathrm{Mat}_{\mathbb{K}}(d^{L-1},d) \xrightarrow{\text{SVD}} U_{\mathbb{K}}(d^{L-1},r_{L-1})\times \mathrm{diag}_{\mathbb{K}}(r_{L-1})\times U_{\mathbb{K}}(r_{L-1},d) \xrightarrow{\cong} \mathrm{Mat}_{\mathbb{K}}(d^{L-2},dr_{L-1})\times(\mathrm{Mat}_{\mathbb{K}}(r_{L-1},1))^d$$

$$\Psi_{(\sigma_1\dots\sigma_{L-1}),\sigma_L} \overset{\text{SVD}}{\longmapsto} = \sum_{a_{L-1}}^{r_{L-1}} U_{(\sigma_1\dots\sigma_{L-1}),a_{L-1}}S_{a_{L-1},a_{L-1}}(V^\dagger)_{a_{L-1},\sigma_L} \overset{\cong}{\longmapsto} \begin{gathered} U_{(\sigma_1\dots\sigma_{L-1}),a_{L-1}}S_{a_{L-1},a_{L-1}} = \Psi_{(\sigma_1\dots\sigma_{L-2}),(\sigma_{L-1}a_{L-1})} \\ (V^\dagger)_{a_{L-1},\sigma_L} = B^{\sigma_L}_{a_{L-1}} \end{gathered}$$

with $\cong$ in this case denoting an isomorphism, the *reshaping* of a matrix into different matrix size dimensions, which should be the inverse of a "flatten" functor, which I'll denote as flatten^{-1} as well (and this is this same isomorphism we're talking about).

Let's deal with the specific procedure of flatten^{-1}, how it reshapes indices in accordance with different matrix size dimensions, and with the so-called "stride" when going from, say, 2-dimensional indices to a "flattened" 1-dimensional index.

Note also as a practical numerical implementation design point, LAPACK's linear algebra BLAS library package and CUBLAS assumes *column*-major ordering.

Consider $i = 1,2,\dots L-1$ (for site i) (or for 0-based counting, starting to count from 0, $i=0,1,\dots L-2$; be aware of this difference as in practical numerical implementation, in C, C++, Python, it assumes 0-based counting).

For a state space of dimension d, we can consider the specific example of $d=2$, representing say a spin-1/2 system. Then index σ_i can be 0 or 1: $\sigma_i \in \{0,1\}$. In general, $\sigma_i \in \{0,1,\dots d-1\}$. I may use d or 2 in the context of the number of states (basis vectors) of the spin system (state vector space).

Consider site i. Suppose the spin system there interacts most with sites $i-1$, $i+1$, and then next sites $i-2$, $i+2$, etc. So the values at $\sigma_{i-1},\sigma_{i+1}$, etc. are most important in calculating interactions with spin system at site i.

Then we seek this reshaping of the matrix index - assuming 0-based counting/ordering, for $l=1$:

$$\{0,1\}^{L-1} \xrightarrow{(\text{flatten})^{-1}} \{0,1,\dots 2^{L-1}-1\}$$

$$(\sigma_0,\sigma_1,\dots\sigma_{L-2}) \overset{(\text{flatten})^{-1}}{\longmapsto} I_{L-1} := \sigma_0 + 2\sigma_1 + \dots + 2^i\sigma_i + \dots + 2^{L-2}\sigma_{L-2} = \sum_{i=0}^{L-2} 2^i\sigma_i$$

In this way, states of a site i are closest in memory addresses in the allocation of a 1-dim. array, on CPU or GPU memory, so that memory access operations should be efficient.

Assuming SVD doesn't change the striding, and defining the result of matrix multiplication:

$$U_{(\sigma_0,\sigma_1\dots\sigma_{L-2}),a_{L-1}}S_{a_{L-1},a_{L-1}} =: (US)_{(\sigma_0\dots\sigma_{L-2}),a_{L-1}} \in \mathrm{Mat}_{\mathbb{K}}(d^{L-1},r_{L-1})$$

We can reshape (i.e. $(\text{flatten})^{-1}$) in such a manner:

$$\text{Mat}_{\mathbb{K}}(d^{L-1}, r_{L-1}) \xrightarrow{(\text{flatten})^{-1}} \text{Mat}_{\mathbb{K}}(d^{L-2}, dr_{L-1})$$

$$(US)_{(\sigma_0 \dots \sigma_{L-2}), a_{L-1}} \xmapsto{(\text{flatten})^{-1}} \Psi_{(\sigma_0, \sigma_1, \dots \sigma_{L-3}), (\sigma_{L-2} a_{L-1})}$$

$$\{0, 1, \dots 2^{L-1} - 1\} \times \{0, 1, \dots r_{L-1} - 1\} \xrightarrow{(\text{flatten})^{-1}} \{0, 1, \dots 2^{L-2} - 1\} \times \{0, 1, \dots dr_{L-1} - 1\}$$

$$I_{L-1}, a_{L-1} \xmapsto{(\text{flatten})^{-1}} I_{L-1} \mod 2^{L-2}, \tfrac{I_{L-1}}{2^{L-2}} + da_{L-1}$$

Reshaping $V^\dagger$ at iteration $l = 1$ can be done as follows:

$$U_{\mathbb{K}}(r_{L-1}, d) \xrightarrow{(\text{flatten})^{-1}} (\text{Mat}_{\mathbb{K}}(r_{L-1}, 1))^d$$

$$(V^\dagger)_{a_{L-1}, \sigma_{L-1}} \xmapsto{(\text{flatten})^{-1}} (V^\dagger)_{a_{L-1}, \sigma_{L-1}} = B^{\sigma_{L-1}}_{a_{L-1}}$$

$$\{0, 1, \dots r_{L-1} - 1\} \times \{0, 1, \dots d - 1\} \xrightarrow{(\text{flatten})^{-1}} (\{0, 1, \dots r_{L-1} - 1\})^d$$

$$a_{L-1}, \sigma_{L-1} \xmapsto{(\text{flatten})^{-1}} a_{L-1}$$

Let's do this same procedure, reshaping or $(\text{flatten})^{-1}$, for a general l iteration.

$$\text{Mat}_{\mathbb{K}}(d^{L-l}, r_{L-l}) \xrightarrow{(\text{flatten})^{-1}} \text{Mat}_{\mathbb{K}}(d^{L-(l+1)}, dr_{L-l})$$

$$(US)_{(\sigma_0 \dots \sigma_{L-(l+1)}), a_{L-l}} \xmapsto{(\text{flatten})^{-1}} \Psi_{(\sigma_0, \sigma_1, \dots \sigma_{L-(l+2)}), (\sigma_{L-(l+1)} a_{L-l})}$$

$$\{0, 1, \dots d^{L-l} - 1\} \times \{0, 1, \dots r_{L-l} - 1\} \xrightarrow{(\text{flatten})^{-1}} \{0, 1, \dots d^{L-(l+1)} - 1\} \times \{0, 1, \dots dr_{L-l} - 1\}$$

$$I_{L-l}, a_{L-l} \xmapsto{(\text{flatten})^{-1}} I_{L-l} \mod d^{L-(l+1)}, \tfrac{I_{L-l}}{d^{L-(l+1)}} + da_{L-l}$$

$$U_{\mathbb{K}}(r_{L-l}, dr_{L-(l-1)}) \xrightarrow{(\text{flatten})^{-1}} (\text{Mat}_{\mathbb{K}}(r_{L-l}, r_{L-(l-1)}))^d$$

$$(V^\dagger)_{a_{L-l}, (\sigma_{L-l} a_{L-(l-1)})} \xmapsto{(\text{flatten})^{-1}} (V^\dagger)_{a_{L-l}, (\sigma_{L-l} a_{L-(l-1)})} = B^{\sigma_{L-l}}_{a_{L-l}, a_{L-(l-1)}}$$

$$\{0, 1, \dots r_{L-l} - 1\} \times \{0, 1, \dots dr_{L-(l-1)} - 1\} \xrightarrow{(\text{flatten})^{-1}} (\{0, 1, \dots r_L - 1\} \times \{0, 1, \dots r_{L-(l-1)} - 1\})^d$$

$$a_{L-l}, (\sigma_{L-l} a_{L-(l-1)}) := a_{L-l}, \sigma_{L-1} + da_{L-(l-1)} \xmapsto{(\text{flatten})^{-1}} a_{L-l}, \tfrac{(\sigma_{L-1} a_{L-(l-1)})}{d}; \sigma_{L-l} = (\sigma_{L-l} a_{L-(l-1)}) \mod d$$

34.3.2. *Numerical implementations of initial states.* Something else that shouldn't be overlooked is the numerical implementation of *initial states*, the c's of a state $|\psi\rangle = \sum_{\{\sigma\}} c^\sigma |\{\sigma\}\rangle$ for a many-body quantum system. Remember what the postulates of quantum mechanics say and interpret accordingly (and correctly). While we call them "probability amplitudes", one should be careful about what physical interpretation we may (or may not!) assign them. One thing's for certain: $c \in \mathbb{C}$ and normalization of the quantum state: $|\langle \psi | \psi \rangle|^2 = 1$

Here are some setups to try:
$d = 2, L = 2, d^L = 2^2 = 4$.

$$\begin{bmatrix} c_{\uparrow\uparrow} & c_{\uparrow\downarrow} & c_{\downarrow\uparrow} & c_{\downarrow\downarrow} \end{bmatrix} \mapsto \begin{bmatrix} c_{\uparrow\uparrow} & c_{\uparrow\downarrow} \\ c_{\downarrow\uparrow} & c_{\downarrow\downarrow} \end{bmatrix}$$

Singlet state: $|\psi\rangle = \frac{1}{\sqrt{2}}|\uparrow\downarrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\uparrow\rangle$, $\begin{bmatrix} 0 & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & 0 \end{bmatrix}$

$d = 2, L = 3, d^L = 2^8 = 8$

For notational convenience, let $\uparrow \equiv 1, \downarrow \equiv 0$

$$\begin{bmatrix} c_{000} & c_{001} & c_{010} & c_{011} & c_{100} & \dots & c_{111} \end{bmatrix} \mapsto \begin{bmatrix} c_{000} & c_{001} & \dots & c_{011} \\ c_{100} & c_{001} & \dots & c_{111} \end{bmatrix}$$

$d = 3, L = 2, d^L = 3^2 = 9$

$$\begin{bmatrix} c_{-1-1} & c_{-10} & c_{-11} & \dots & c_{11} \end{bmatrix} \mapsto \begin{bmatrix} c_{-1-1} & c_{-10} & c_{-11} \\ c_{0-1} & c_{00} & c_{01} \\ c_{1-1} & c_{10} & c_{11} \end{bmatrix}$$

Part 11. **Algebraic Geometry**

35. Affine and Projective Varieties

cf. Harris (1992)[27]

For (algebraically closed) field K,
vector space K^n,
affine space $\mathbb{A}^n_K \equiv \mathbb{A}^n = K^n$, but origin plays no special role in affine space.
Affine variety $X \subset \mathbb{A}^n :=$ common zero locus of collection of polynomials $f_\alpha \in K[z_1 \dots z_n] :=$

$$X = \{Z | f_\alpha(Z) = 0 \quad \forall \alpha, \quad f_\alpha \in K(z_1 \dots z_n), Z = (z_1 \dots z_n)\}$$

35.1. **Projective Space and Projective Varieties.** Projective space over field K = set of 1-dim. subspaces of vector space $K^{n+1} \equiv \mathbb{P}^n_K \equiv \mathbb{P}^n = (K^{n+1} - \{0\})/K^*$,
where $(K^{n+1} - \{0\})/K^*$ is the quotient of $K^{n+1} - \{0\}$ by the action of the group K^n acting by scalar multiplication.

$\mathbb{P}(V) \equiv \mathbb{P}V \equiv$ projective space of 1-dim. subspaces of a vector space V over field K.

$P \in \mathbb{P}^n$ usually written as homogeneous vector $[Z_0 \dots Z_n]$, by which be mean line spaced by $(Z_0 \dots Z_n) \in K^{n+1}$.

For U_n s.t. $\forall P \in U_n \subset \mathbb{P}^n \subset V^{n+1}$, $Z_n \neq 0$. Then $[Z_0 \dots Z_n] \sim \left[\frac{Z_0}{Z_n}, \dots, \frac{Z_{n-1}}{Z_n}, 1 \right] \cong \left[\frac{Z_0}{Z_n}, \dots \frac{Z_{n-1}}{Z_n} \right] \in K^n$.

$\forall v \neq 0$, $v \in V$, $[v]$ = corresponding pt. in $\mathbb{P}V \cong \mathbb{P}^n$

Polynomial $F \in K[Z_0 \dots Z_n]$ on vector space K^{n+1} doesn't define a function on $\mathbb{P}^n$, but
if F is homogeneous of degree d,
then since
$$F(\lambda Z_0, \dots, \lambda Z_n) = \lambda^d F(Z_0 \dots Z_n)$$
it does make sense to talk about 0 locus of polynomial F.

Definition 80 (Projective variety). *projective variety* $X \subset \mathbb{P}^n = \{ P | F_\alpha(P) = 0 \, \forall \alpha, \; F_\alpha(\lambda P) = \lambda^d F_\alpha(P) \}$ *= zero locus of a collection of homogeneous polynomials* F_α.

Group $PGL_{n+1}K$ acts on space $\mathbb{P}^n$ (in Lecture 18, $PGL_{n+1}K$ are automorphisms of $\mathbb{P}^n$).
Varieties $X, Y \subset \mathbb{P}^n$ are projectively equivalent, if they're congruent, modulo this group.
Note that if $\mathbb{P}^n = \mathbb{P}V$ is projective space associated with vector space V,

- homogeneous coordinates on $\mathbb{P}V$ correspond to elements of dual space V^*
- similarly, space of homogeneous polynomials of degree d on $\mathbb{P}V$ naturally identified with vector space $\text{Sym}^d(V^*)$

Meaning, set of linear coordinates on vector space V, dim$V = n$, over field K (so $V = K^n$), $\alpha_i \equiv z_i$, $i = 1 \dots n$, is a *basis* (α_i) of V^*, since
$$\begin{aligned} \alpha : V &\to K^n \\ v &\mapsto (\alpha_1(v), \dots \alpha_n(v)) \end{aligned} \quad \text{i.e.} \quad \equiv \quad \begin{aligned} z : V &\to K^n \\ v &\mapsto (z_1(v) \dots z_n(v)) \end{aligned}$$

Now $\mathbb{P}(V) = (V \backslash \{0\})/K^*$ and homogeneous coordinates on $\mathbb{P}(V)$ are just linear coordinates on V up to action K^*

cf. "Correspondence between the projective space associated to a vector space and the dual space of the vector space?", stackexchange, Can dual vector spaces be thought of as linear coordinate functions? stackexchange

From $Z_i \in V^*$, $i = 0, 1 \dots n$, $Z_i : V \to K$, $Z_i : v \mapsto Z_i(v) = Z_i \in K$,
let f be a homogeneous polynomial of degree d on $\mathbb{P}V$:
$$f = \sum a_{i_0 i_1 \dots i_n} z_0^{i_0} z_1^{i_1} \dots z_n^{i_n}$$
where summation $\sum$ is over $0 \leq i_0, i_1, \dots i_n \leq d$ s.t. $\sum_{j=0}^n i_j = d$.

$\text{dimSym}^d(V^*) = \binom{d+n}{n}$

$\{ z_0^{i_0} z_1^{i_1} \dots z_n^{i_n} \}_{\substack{0 \leq i_0, i_1 \dots i_n \leq d \\ \sum_{j=0}^n i_j = d}}$ form a basis for $\text{Sym}^d(V^*)$

Let $U_i \subset \mathbb{P}^n$, $U_i = \{ [Z_0 \dots Z_n] | Z_i \neq 0 \}$. Then $[Z_0 \dots Z_n] \sim \left[\frac{Z_0}{Z_i} \dots \frac{Z_{i-1}}{Z_i}, 1 \dots \frac{Z_n}{Z_i} \right] \equiv [z_0, \dots z_{i-1}, 1, z_i \dots z_{n-1}] \cong (z_0, z_1 \dots z_{n-1}) \in K^n$.

So there's a bijection $U_i \to K^n$.

Geometrically, this map is associating line $L \subset K^{n+1}$ not contained in hyperplane $(Z_i = 0)$, its pt. p of intersection with affine plane $(Z_i = 1) \subset K^{n+1}$.

Coordinates z_j on U_i are called affine or Euclidean coordinates on projective space or open set U_i
- open sets U_i comprise standard cover of $\mathbb{P}^n$ by affine open sets.

If $X \subset \mathbb{P}^n$ is a variety, $X_i = X \cup U_i$ is affine variety:
if X given by polynomials $F_\alpha \in K[Z_0, \dots Z_n]$, then e.g. X_0 will be zero locus of polynomials
$$f_\alpha(z_0 \dots z_n) = F_\alpha(Z_0 \dots Z_n)/Z_0^d = F_\alpha(1, z_1 \dots z_n)$$
where $d = \deg F_\alpha$.

For (projective) variety $X \subset \mathbb{P}^n$, $X = \{ P | F_\alpha(P) = 0, \forall \alpha, F_\alpha \text{ homogeneous}, \, P = [Z_0, Z_1 \dots Z_n] \in \mathbb{P}^n \}$,
obtain affine variety $X_i = X \cup U_i$ as follows: for
$$z_j = \begin{cases} \frac{Z_{j-1}}{Z_i} & j \leq i \\ \frac{Z_j}{Z_i}, & j > i \end{cases}$$
$$f_\alpha(z_1 \dots z_n) = f_\alpha \left(\frac{Z_0}{Z_i}, \dots \frac{Z_{i-1}}{Z_i}, \frac{Z_{i+1}}{Z_i} \dots \frac{Z_n}{Z_i} \right) = \frac{1}{Z_i}^{d_\alpha} F_\alpha(Z_0 \dots Z_n) = F_\alpha(z_1 \dots z_i, 1, z_{i+1}, \dots z_n)$$
If $F_\alpha(Z_0 \dots Z_n) = 0$, then $f_\alpha(z_1 \dots z_n) = 0$

$\forall$ projective variety X, X is union of affine varieties.

If affine variety $X_i \subset K^n \cong U_i \subset \mathbb{P}^n$, by def. X_i given by polynomials $\{ f_\alpha \}_\alpha$
$$f_\alpha(z_1 \dots z_n) = \sum a_{i_1 \dots i_n} z_1^{i_1} \dots z_n^{i_n} = 0$$
of degree d_α (i.e. $i_1 + \dots i_n = d_\alpha$)

Then
$$F_\alpha(Z_0 \dots Z_n) = Z_i^{D_\alpha} F_\alpha \left(\frac{Z_0}{Z_i} \dots \frac{Z_n}{Z_i} \right) = Z_i^{D_\alpha} f_\alpha(z_1 \dots z_n) = \sum a_{i_1 \dots i_n} Z_i^{D_\alpha - \sum i_l} Z_0^{i_0} \dots Z_n^{i_n} =$$
$$= \sum a_{i_1 \dots i_n} Z_i^{D_\alpha - d_\alpha} Z_0^{i_0} \dots \widehat{Z}_i^{i_i} \dots Z_n^{i_n}$$

35.1.1. *Example: ellipse.*
$$\mathbb{P}^n \to U_Z \cong K^n$$
$$[X, Y, Z] \mapsto (x, y) = \left(\frac{X}{Z}, \frac{Y}{Z} \right) \tag{102}$$
Consider
$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \text{ or } f(x, y) = \frac{x^2}{a^2} + \frac{y^2}{b^2} - 1 \tag{103}$$
For affine variety $X_Z \subset K^2$,
$$F(X, Y, Z) = \left(\frac{X^2}{Z^2 a^2} + \frac{Y^2}{Z^2 b^2} - 1 \right) Z^2 = \frac{X^2}{a^2} + \frac{Y^2}{b^2} - Z^2 \tag{104}$$

36. Algebraic Curves; Conic sections

cf. Reid (2013) [26].
cf. Ch. 0 "Woffle" of Reid (2013) [26].
Given field k, $k[x_1 \dots x_n]$ colelction of all polynomials in $x_1 \dots x_n$, with coefficients in k,
$$f \in k[x_1 \dots x_n] = \{ f | f = \sum_\alpha c_\alpha x^\alpha, x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}, \, c_\alpha \in k \}$$
Variety is (roughly) locus defined by polynomial equations
$$V = \{ P \in k^n | f_i(P) = 0 \} \subset k^n, \, f_i \in k[x_1 \dots x_n]$$
e.g. plane curves C: $(f(x, y) = 0) \subset \mathbb{R}^2$ or $\mathbb{C}^2$

Groups of transformations (i.e. transformation groups) are of central importance throughout geometry; properties of geometric figures must be invariant under appropriate kind of transformations before they're significant.

affine change of coordinates in $\mathbb{R}^2$ is of form
$$T(\mathbf{x}) = A\mathbf{x} + B \quad \text{(affine change of coordinates)} \tag{105}$$
where $\mathbf{x} = (x, y) \in \mathbb{R}^2$, A 2×2 invertible matrix (i.e. $A \in GL(2, \mathbb{R})$), $B \in \mathbb{R}^2$.

If A orthogonal, transformation T is *Euclidean.*

$\forall$ nondegenerate conic can be reduced to "standard form" by Euclidean transformation.

projectivity or projective transformation $\mathbb{P}^2_{\mathbb{R}}$ is map $T(\mathbf{X}) = M\mathbf{X}$, $M \in GL(3,\mathbb{R})$.

Understand T on affine piece $\mathbb{R}^2 \subset \mathbb{P}^2_{\mathbb{R}}$ is partially defined map $\mathbb{R}^2 \to \mathbb{R}^2$; it's a fractional linear transformation.

$$(x,y) \xmapsto{\cong} [x,y,1]$$
$$(x,y) \mapsto \begin{pmatrix} A\begin{pmatrix} x \\ y \end{pmatrix} + B \\ cx+dy+e \end{pmatrix}$$

where

$$M = \left(\begin{array}{c|c} A & B \\ c \quad d & e \end{array} \right)$$

e.g. 2 different photographs of same (plane) object are obviously related by a projectivity.

For inhomogeneous quadratic polynomial q, homogeneous quadratic polynomial Q, then there exists bijection

$$q \in K[x,y] \xmapsto{\cong} Q \in K[X,Y,Z]$$
$$q(x,y) = ax^2 + bxy + cy^2 + dx + ey + f \mapsto Q(X,Y,Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2$$

so

$$q(x,y) = Q\left(\frac{X}{Z}, \frac{Y}{Z}, 1 \right) \text{ with } x = X/Z,\ y = Y/Z$$

inverse:

$$Q = Z^2 q(X/Z, Y/Z)$$

36.0.1. *"Line at infinity" and asymptotic directions.* cf. Ch. 1 of Reid (2013)

Points of $\mathbb{P}^2$ with $Z = 0$, $[X,Y,0]$, form *line at infinity*, a copy of $\mathbb{P}^1_{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ (since $[X,Y] \mapsto X/Y$) define bijection $\mathbb{P}^1_{\mathbb{R}} \to \mathbb{R} \cup \{\infty\}$.

Line in $\mathbb{P}^2$, L, $L := \{[X,Y,Z] | aX + bY + cZ = 0\}$.

L passes through $(X,Y,0) \Longleftrightarrow aX + bY = 0$.

(a) hyperbola $\left(\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \right)$. Recall that the lines of asymptotes (asymptotic lines). They are found in the following manner:
$$\frac{(bx-ay)(bx+ay)}{a^2b^2} = 1 \text{ or } \frac{bx-ay}{a^2b^2} = \frac{1}{bx+ay} \xrightarrow{x,y \to \infty} \frac{bx-ay}{a^2b^2} = 0 \text{ or } y = \frac{b}{a}x$$
Now, $\left(\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \right)$ in $\mathbb{R}^2$ corresponds in $\mathbb{P}^2_{\mathbb{R}}$ to $C : \left(\frac{X^2}{a^2} - \frac{Y^2}{b^2} = Z^2 \right)$.
This meets $(Z = 0)$ in 2 pts. $(a, \pm b, 0) \in \mathbb{P}^2_{\mathbb{R}}$, corresponding to asymptotic lines of hyperbola, $y = \frac{b}{a}x$, $y = \frac{-b}{a}x$
For affine piece $U_x \subset \mathbb{P}^2_{\mathbb{R}}$, $U_x = \{p \in \mathbb{P}^2_{\mathbb{R}} | p = [X,Y,Z] \text{ s.t. } X \neq 0\}$, then bijection $U_x \to \mathbb{R}^2$,
$$[X,Y,Z \sim [1, \frac{Y}{X}, \frac{Z}{X}] \mapsto (u,v) = \left(\frac{Y}{X}, \frac{Z}{X} \right), \text{ so}$$
$$C : X^2/a^2 - Y^2/b^2 = Z^2 \mapsto u^2 + \frac{v^2}{b^2} = \frac{1}{a^2} \text{ or } \frac{u^2}{1/a^2} + \frac{v^2}{(b/a)^2} = 1 \qquad \text{(an ellipse!)}$$

(b) $y = mx^2$ (parabola) in $\mathbb{R}^2 \mapsto C : YZ = mX^2$ in $\mathbb{P}^2_{\mathbb{R}}$.
For $Z = 0$, C meets $Z = 0$ at single pt. $[0,1,0] \sim [0,Y,0]$. So in $\mathbb{P}^2$, "2 branches of parabola meet at infinity."

36.0.2. *Classification of conics in $\mathbb{P}^2$.* cf. 1.6. Classification of conics in $\mathbb{P}^2$, Reid (2013) [26]

Let K be any field of characteristic $\neq 2$.

Recall 2 linear algebra results for quadratic forms:

Proposition 21. *$\exists$ bijections*
$\{$ *homogeneous quadratic polynomials* $\} = \{$ *quadratic forms* $K^3 \to K$ $\} \cong \{$ *symmetric bilinear forms on* K^3 $\}$ *given by*

$$aX^2 + 2bXY + cY^2 + 2dXZ + 2eYZ + fZ^2 \cong \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix} \text{ since}$$
$$\begin{bmatrix} X & Y & Z \end{bmatrix} \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = aX^2 + 2bXY + cY^2 + 2dXZ + 2eYZ + fZ^2$$

Quadratic form nondegenerate if corresponding bilinear form nondegenerate, i.e. matrix is nonsingular.

Theorem 15. *Let V be vector space over K, quadratic form $Q : V \to K$, then $\exists$ basis of V s.t.*

$$Q = \epsilon_1 x_1^2 + \epsilon_2 x_2^2 + \dots + \epsilon_n x_n^2 \text{ with } \epsilon_i \in K \tag{106}$$

This theorem is proved by Gram-Schmidt orthogonalization.

For $\lambda \in K \backslash \{0\}$, $x_i \mapsto \lambda x_i$ takes $\epsilon_i \mapsto \lambda^{-2}\epsilon_i$.

Corollary 3. *In a suitable coordinate system, any conic in $\mathbb{P}^2$ is one of*

(a) *nondegenerate conic* $C : (X^2 + Y^2 - Z^2 = 0)$

36.0.3. *Parametrization of a conic.* Let C be a nondegenerate, nonempty conic of $\mathbb{P}^2_{\mathbb{R}}$.

Then by Corollary 3 (cf. Corollary 1.6 (cf. Reid (2013) [26]), and taking new coordinates $[X+Z, Y, Z-X]$,

$$X^2 + Y^2 - Z^2 = 0 \mapsto (X+Z)^2 + Y^2 - (Z-X)^2 = X^2 + 2XZ + Z^2 + Y^2 - (Z^2 - 2ZX + X^2) = Y^2 + 4XZ = 0$$

$\Longrightarrow C$ is projectively equivalent to curve $(Y^2 = XZ)$.

This is a curve parametrized by

$$\Phi : \mathbb{P}^1_{\mathbb{R}} \to C \subset \mathbb{P}^2_{\mathbb{R}}$$
$$[U,V] \mapsto [U^2, UV, V^2]$$

This is because

$$[X,Y,Z] \sim [X^2, XY, XZ] = [X^2, XY, Y^2]$$

and so let $U = X, V = Y$. Note that if $X \mapsto X + Z$, then $U = X + Z$.

Inverse map $\Psi = \Phi^{-1}$, $\Psi : C \to \mathbb{P}^1_{\mathbb{R}}$ given by

$$[X,Y,Z] \mapsto [X,Y] = [Y,Z]$$

$[X,Y]$ defined if $X \neq 0$, $[Y,Z]$ defined if $Z \neq 0$.

Φ, Ψ are inverse isomorphisms of varieties.

cf. Ch. 2 "Cubics and the group law" of Reid (2013) [26].

cf. Sec. 2.1 "Examples of parametrized cubics" in Ch. 2 of Reid (2013) [26].

Nodal cubic: $C : (y^2 = x^3 + x^2) \subset \mathbb{R}^2$, is image of map $\varphi : \mathbb{R}^1 \to \mathbb{R}^2$, $t \mapsto (t^2 - 1, t^3 - t)$, since

$$(t^2-1)^3 + (t^2-1)^2 = t^6 - 3t^4 + 3t^2 - 1 + t^4 - 2t^3 + 1 = t^6 - 2t^4 + t^2 = t^2(t^4 - 2t^2 + 1) = t^2(t^2-1)^2 = y^2$$

Cuspidal cubic $C : (y^2 = x^3) \subset \mathbb{R}^2$ is image of $\varphi : \mathbb{R}^1 \to \mathbb{R}^2$, $t \mapsto (t^2, t^3)$

36.0.4. *Curve $y^2 = x(x-1)(x-\lambda)$ has no rational parametrization.* cf. Sec. 2.2 "Curve $y^2 = x(x-1)(x-\lambda)$" in Ch. 2 of Reid (2013) [26].

$f = f(t)$ *rational function* if it's a quotient of 2 polynomials.

Lemma 2. *Let $\overline{K}$ algebraically closed field, $p, q \in \overline{K}[t]$ coprime elements (i.e. if $\exists x$ s.t. p/x, $q/x \in \overline{K}$ (i.e. $x|p$, $x|q$), then $x = 1$),*
assume 4 distinct linear combinations (i.e. $\lambda p + \mu q$ for 4 distinct ratios $(\lambda : \mu) \in \mathbb{P}^1 K$) are squares in $\overline{K}[t]$,
then $p, q \in \overline{K}$

cf. Lemma 2.3 of Reid (2013) [26]

Proof. (Fermat's method of "infinite descent")
Without loss of generality,

$$p' = ap + bq$$
$$q' = cp + dq$$

$a, b, c, d \in K$, $ad - bc \neq 0$.
Hence, assume 4 given squares are

$$p, p-q, p-\lambda q, q$$

i.e. $\lambda p + \mu q$, for $\lambda = 1, \mu = 0$; $\lambda = 1, \mu = -1$; $\lambda = 1, \mu = -\lambda$; $\lambda = 0, \mu = 1$
Since a, b, c, d arbitrary linear transformation.
Then $p = u^2, q = v^2$, $u, v \in \overline{K}[t]$ are coprime, with

$$\max(\deg u, \deg v) < \max(\deg p, \deg q)$$

Suppose $\max(\deg p, \deg q) > 0$ and is minimal among all p, q satisfying lemma condition.
Then

$$p - q = u^2 - v^2 = (u-v)(u+v)$$
$$p - \lambda q = u^2 - \lambda v^2 = (u - \mu v)(u + \mu v)$$

where $\mu = \sqrt{\lambda}$, are squares in $\overline{K}[t]$.
So by u, v being coprime,
Then $u - v, u + v, u - \mu v, u + \mu v$ are squares.
This contradicts minimality of $\max(\deg p, \deg q)$

□

Theorem 16 ($y^2 = x(x-1)(x-\lambda)$ has no rational parametrization)**.** *Let K be field of characteristic $\neq 2$, let $\lambda \in K$, $\lambda \neq 0, 1$; let $f, g \in K(t)$ be rational functions s.t.*

$$f^2 = g(g-1)(g-\lambda)$$

Then $f, g \in K$.

EY (20181229). Recall, *characteristic of ring R* (e.g. field), $\text{char}(K)$, smallest number of times 1 must using ring's multiplicative identity 1 in a sum to get additive identity (0).
$\text{char}(K) = 0$ for case that $\underbrace{1 + \dots + 1}_{n} = \sum_{i=1}^n 1 \neq 0 \quad \forall n \in \mathbb{Z}^+$.
Theorem 16 is equivalent to $\nexists$ nonconstant map $\mathbb{R}^1 \to C : (y^2 = x(x-1)(x-\lambda))$ given by rational functions.

Proof. $K[t]$ UFD; unique factorization domain (given).
EY: 20181229, recall the definitions: integral domain - nonzero cummutative ring in which product of any 2 nonzero elements is nonzero.
unique factorization domain is an integral domain R s.t. $\forall x \in R$, $x \neq 0$, x can be written as

$$x = up_1 p_2 \dots p_n, \quad n \geq 0$$

with irreducible elements p_i of R, unit u.

$$\Longrightarrow \begin{aligned} & f = r/s && r, s \in K[t] \text{ and coprime} \\ & g = p/q && p, q \in K[t] \text{ and coprime} \end{aligned}$$

$$\Longrightarrow f^2 = g(g-1)(g-\lambda) = \frac{r^2}{s^2} = \frac{p}{q}\left(\frac{p-q}{q}\right)\left(\frac{p-\lambda q}{q}\right) \Longrightarrow r^2 q^3 = s^2 p(p-q)(p-\lambda q)$$

r, s are coprime, so RHS s^2 must divide q^3.
p, q are coprime, LHS q^3 must divide s^2
EY (20181229): observe that LHS and RHS are different and equal. How to get them into the same form? Try to divide both sides!

$$\Longrightarrow s^2 | q^3 \text{and } q^3 | s^2, \text{ so } s^2 = aq^3 \text{ with } a \in K$$

Then $aq = (s/q)^2$ is square in $K[t]$
Then $r^2 = ap(p-q)(p-\lambda q)$
Consider factorization into primes $\Longrightarrow$ nonzero constants $b, c, d \in K$, s.t. $bp, c(p-q), d(p-\lambda q)$ are all squares in $K[t]$.
Let algebraic closure $\overline{K}$ (algebraic extension of K s.t. $\overline{K}$ algebraically closed, i.e. $\forall$ nonconstant $f(x) \in K[x]$ has a root in K).
Then $\forall p, q \in \overline{K}(t)$, by lemma, $p, q \in \overline{K}$. Then $r, s \in \overline{K}$. Then $\boxed{f, g \in \overline{K}}$.

□

cf. Sec. 2.4 "Linear systems" in Ch. 2 of Reid (2013) [26].
Let $S_d \equiv \{$ forms of degree d in (X, Y, Z) $\}$; recall form is just a homogeneous polynomial.
$\forall F \in S_d$, $\exists$ unique form for F: $F = \sum a_{ijk} X^i Y^j Z^k$, $a_{ijk} \in K$, and $\sum \equiv \sum_{\substack{i,j,k \geq 0 \\ i+j+k=d}}$.
$\Longrightarrow S_d$ is K-vector space with basis $\{Z^d, XZ^{d-1}, YZ^{d-1}, \dots X^{d-2}Y^2 \dots Y^d\}$, where

$$\boxed{\dim S_d = \binom{d+2}{2}}$$

(to see this, imagine d stars, 2 bars, and the 2 bars distinguish which are X's, Y's, or Z's).
For $P_1 \dots P_n \in \mathbb{P}^2$, let

$$S_d(P_1 \dots P_n) = \{F \in S_d | F(P_i) = 0 \quad \forall i = 1 \dots n\} \subset S_d$$

$\forall$ condition $F(P_i) = 0$ (e.g. $F(X_i, Y_i, Z_i) = 0$, where $P_i = (X_i, Y_i, Z_i)$) is 1 linear condition on F, so $S_d(P_1 \dots P_n)$ is a vector space of dim $\geq \binom{d+2}{2} - n$

Lemma 3 (Special case of Nullstellensatz)**.** (i) *Let $L \subset \mathbb{P}^2_K$ be a line; if $F \equiv 0$ on L, then F divisible in $K[X, Y, Z]$ by equation of L, i.e. $F = H \cdot F'$, where H is equation of L, and $F' \in S_{d-1}$.*
(ii) *Let $C \subset \mathbb{P}^2_K$ be nonempty nondegenerate conic; if $F = 0$ on C, then F divisible in $K[X, Y, Z]$, by equation of C, i.e. $F = QF'$, where Q is equation of C, and $F' \in S_{d-2}$.*

cf. Lemma 2.5 of Reid (2013).

Proof. (i) By change of coordinates, assume $H = X$, Then, $\forall F \in S_d$, $\exists ! F = X \cdot F'_{d-1} + G(Y, Z)$, since, just gather together all monomials involving X into 1st. summand, and what's left must be a polynomial Y, Z.
Since
$F = 0$ on L, $F(0) = 0 = 0 \cdot F'_{d-1} + G(Y, Z) \Longrightarrow G(Y, Z) = 0 \quad \forall Y, Z$.
Otherwise, if $G(Y, Z) \neq 0$, then it has at most d zeros on $\mathbb{P}^1_K$, whereas if K is infinite, then so is $\mathbb{P}^1_K$.
(ii) By change of coordinates $Q = XZ - Y^2$,
Consider why

$$F = QF'_{d-2} + A(X, Z) + YB(X, Z)$$

where $d - 2$ in F'_{d-2} denotes the *degree* of the polynomial (to be $d - 2$).

This is because if $Y^2 = XZ - Q$, then $F(Y^2 = XZ - Q)$ has degree ≤ 1 in Y, and so would have the form

$$F(Y^2 = XZ - Q) = A(X, Z) + YB(X, Z)$$

C is a parametrized conic given by

$$X = U^2, Y = UV, Z = V^2$$

so that,
$F = 0$ on $C \iff A(U^2, V^2) + UVB(U^2, V^2) = 0$ on C
$\implies A(U^2, V^2) + UVB(U^2, V^2) = 0 \in K[U, V]$.
$\implies A(X, Z) = B(X, Z) = 0$

Since here the last equality comes by considering separately terms of even and odd degrees in form

$$A(U^2, V^2) + UVB(U^2, V^2)$$

□

cf. Exercises to Ch. 2, Reid (2013)

Exercise 2.2. Let $\varphi : \mathbb{R}^1 \to \mathbb{R}^2$.

$t \mapsto (t^2, t^3)$

$\forall$ polynomial $f \in \mathbb{R}[X, Y]$, s.t. $f = 0$ on image $C = \varphi(\mathbb{R}^1)$, f divisible by $Y^2 - X^3$.

Proof. Given $\varphi(t) = (t^2, t^3) = (x, y)$, then $y^2 = x^3 \quad \forall t \in \mathbb{R}$, or $y^2 - x^3 = 0$.
Let $q = q(x, y) = y^2 - x^3 \in K[x, y]$.
Suppose f of degree d.
Then

$$f = qf'_{d-2} + a(x) + yb(x)$$

This is because, if $y^2 = q - x^3$, $f(y^2 = q - x^3)$ has degree ≤ 1 in y, so would have the previous form.
Now

$$f(y^2 = q - x^3) = 0 = 0 + a(x) + yb(x)$$

$f = 0$ on $C = \varphi(\mathbb{R}^1) \implies a(x) + yb(x) = 0 = a(t^2) + t^3 b(t^2) = 0$.
Suppose for $t_1 > 0$, $t_1^3 b(t_1^2) = -a(t_1^2)$.
Consider $-t_1 < 0$:

$$\implies -t_1^3 b(t_1^3) = -a(t_1^2) \implies a(t_1^2) = 0 \quad \forall t_1 > 0$$

Then $b(t_1^2) = 0 \; \forall t_1 > 0$.
$\implies f = qf'_{d-2}$ where $q = y^2 - x^3$.
K needs to have "negative numbers" (i.e. additive inverses) to exist, for this proof to work. □

References

[1] Masaki Kashiwara and Pierre Schapira. **Categories and Sheaves**. *Grundlehren der mathematischen Wissenschaften.* Volume 332. 2006. Springer-Verlag Berlin Heidelberg. eBook ISBN 978-3-540-27950-1
[2] David S. Dummit, Richard M. Foote. **Abstract Algebra**. 3rd. Ed. Wiley; (July 14, 2003). ISBN-13: 978-0471433347
[3] Michael Barr, Charles Wells. **Category Theory for Computing Science**. http://www.tac.mta.ca/tac/reprints/articles/22/tr22.pdf, http://www.math.mcgill.ca/triples/Barr-Wells-ctcs.pdf
[4] Jiří Adámek, Horst Herrlich, George E. Strecker. **Abstract and Concrete Categories The Joy of Cats**. 2004. http://katmat.math.uni-bremen.de/acc/acc.pdf
[5] David A. Cox. John Little. Donal O'Shea. **Using Algebraic Geometry**. Second Edition. Springer. 2005. ISBN 0-387-20706-6 QA564.C6883 2004
[6] David Cox, John Little, Donal O'Shea. **Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra**, Fourth Edition, Springer
[7] Franz Schwabl. **Quantum Mechanics**. Springer-Verlag Berlin Heidelberg. 2007. 4th Edition. ISBN 978-3-540-71933-5
[8] Schottenloher, Martin. **A Mathematical Introduction to Conformal Field Theory**. Springer, 2008.
[9] L.D. Landau and E.M. Lifshitz. **Statistical Physics**, Third Edition, Part 1: Volume 5 (Course of Theoretical Physics, Volume 5) 3rd Edition. Butterworth-Heinemann; 3 edition (January 15, 1980). ISBN-13: 978-0750633727
[10] M. Hjorth-Jensen, **Computational Physics**, University of Oslo (2015) http://www.mn.uio.no/fysikk/english/people/aca/mhjensen/
[11] M.E.J. Newman and G.T. Barkema. **Monte Carlo Methods in Statistical Physics**. Oxford University Press. 1999.
[12] Glen E. Bredon. **Topology and Geometry**. Graduate Texts in Mathematics (Book 139). Springer; Corrected edition (October 17, 1997). ISBN-13: 978-0387979267
[13] Jean-Pierre Serre (Author), J. Stilwell (Translator). **Trees** (Springer Monographs in Mathematics) 1st ed. 1980. Corr. 2nd printing 2002 Edition. ISBN-13: 978-3540442370
[14] Joseph J. Rotman, **Advanced Modern Algebra** (Graduate Studies in Mathematics) 2nd Edition, American Mathematical Society; 2 edition (August 10, 2010), ISBN-13: 978-0821847411
[15] Edward Scheinerman. **C++ for Mathematicians: An Introduction for Students and Professionals**. 1st Edition. CRC Press; 1 edition (June 8, 2006). ISBN-13: 978-1584885849
[16] Jeffrey M. Lee. **Manifolds and Differential Geometry**, *Graduate Studies in Mathematics* Volume: 107, American Mathematical Society, 2009. ISBN-13: 978-0-8218-4815-9
[17] Jacob C. Bridgeman and Christopher T. Chubb. *Hand-waving and Interpretive Dance: An Introductory Course on Tensor Networks: **Lecture Notes**.* arXiv:1603.03039 **[quant-ph]**
[18] Ulrich Schollwoeck. *The density-matrix renormalization group. Rev. Mod. Phys.* **77**, 259 (2005) arXiv:cond-mat/0409292 **[cond-mat.str-el]**
[19] Ulrich Schollwoeck. *The density-matrix renormalization group in the age of matrix product states. Annals of Physics* **326**, 96 (2011). arXiv:1008.3477 **[cond-mat.str-el]**
[20] Ulrich Schollwöck, et. al. *Numerical methods for correlated many-body systems.* **2017 Arnold Sommerfeld School**.
Matrix product states (MPS), Density matrix renormalization group (DMRG) Lecture 1
Matrix product states (MPS), Density matrix renormalization group (DMRG) Lecture 2
Matrix product states (MPS), Density matrix renormalization group (DMRG) Hands on Session 1
Matrix product states (MPS), Density matrix renormalization group (DMRG) Hands on Session 2
Ulrich Schollwöck (LMU): *Matrix product states (MPS), Density matrix renormalization group (DMRG)*
Ulrich Schollwöck (LMU): *Matrix product states (MPS), Density matrix renormalization group (DMRG)*
[21] José L.F. Barbón and Eliezer Rabinovici. "Holographic Complexity And Spacetime Singularities." arXiv:1509.09291 **[hep-th]**
[22] Juan Maldacena, Leonard Susskind. "Cool horizons for entangled black holes." arXiv:1306.0533 **[hep-th]**
[23] Slava Rychkov. "EPFL Lectures on Conformal Field Theory in $D \geq 3$ Dimensions." arXiv:1601.05000 **[hep-th]**
[24] G. Evenbly, G. Vidal. "Tensor network states and geometry." arXiv:1106.1082 **[quant-ph]**
[25] Mark Van Raamsdonk. "Lectures on Gravity and Entanglement." arXiv:1609.00026 **[hep-th]**
[26] Miles Reid. **Undergraduate Algebraic Geometry**. October 20, 2013. https://homepages.warwick.ac.uk/staff/Miles.Reid/MA4A5/UAG.pdf
[27] Joe Harris. **Algebraic Geometry: A First Course**. Graduate Texts in Mathematics. 1992. Springer-Verlag New York. eBook ISBN 978-1-4757-2189-8