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

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) [10].

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

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) [10]

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

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) [10]

Definition 1 (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) [10]

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

Definition 2 (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) [10]

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.*

$$d = sa + tb \tag{1}$$

cf. pp.4, Thm. 1.7, Ch. 1 Things Past of Rotman (2010) [10]

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) [10])**.** *If p prime and $p|ab$, then $p|a$ or $p|b$.*
More generally,
if prime p divides product $a_1a_2\dots a_n$,
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. $a_1a_2\dots a_n/p\in\mathbb{Z}$,
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) [10])**.** *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) [10].

Proof. □

Definition 3. *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) [10]

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,

$$\boxed{\begin{gathered} a \equiv b \bmod m \\ \text{meaning} \\ \frac{a-b}{N} \in \mathbb{Z} \text{ or } a-b = kN, \; k \in \mathbb{Z} \text{ or } a = b+kN \end{gathered}} \tag{2}$$

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 $\begin{matrix} a-b = kN \\ b-c = lN \end{matrix}$, then $a - c = (k+l)N$.

cf. Prop. 1.19 of Rotman (2010) [10]

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, $a = q_a m + r_a$, $\quad 0 \leq r_a < |m|$. $\frac{a - r_a}{m} = q_a \in \mathbb{Z}$ so let $b = r_a$. □

Theorem 5 (1.26 of Rotman (2010) [10])**.** *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) [11])**.** *Let $a, b \in \mathbb{Z}$, let $c = a \bmod b$, i.e. $a = qb + c$ s.t. $0 \leq c < b$. Then*

$$gcd(a, b) = gcd(b, c) \tag{3}$$

cf. Sec. 3.3 Euclid's method of Scheinerman (2006) [11]

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) [11]
For

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

$$\text{that are relative prime to}$$
$$n = |\{i | i \in \{1, 2, \dots n\}, (n, i) = 1 \text{ or equivalently } n \propto i\}|$$

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. $1 \le n \le 77$.

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

By Prop. 3,

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

Scheinerman (2006) [11]
cf. Ex. 1.19, pp. 13, Sec. 1.1 Some Number Theory of Rotman (2010) [10] **Exercise 1.19.** If a and b are relativel prime and if each divides an integer n, then their product ab also divides n, i.e.

Theorem 6. *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 7. *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).

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

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

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

$$\begin{aligned} x &\equiv a \bmod m \qquad & y &\equiv a \bmod m \\ x &\equiv b \bmod n \qquad & y &\equiv b \bmod n \end{aligned}$$

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. 6.
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) [10], pp. 68 Thm. 5.2 (Chinese Remainder) of Scheinerman (2006) [11].

2. Groups; normal subgroups

Definition 4 (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 5 (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 6 (exact sequence of groups)**.** ***exact sequence*** *if $imf_{n+1} = kerf_n \quad \forall\, n$ for sequence of group homomorphisms and groups*

$$G_{n+1} \xrightarrow{f_{n+1}} G_n \xrightarrow{f_n} G_{n-1} \tag{4}$$

Theorem 8. (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, $\text{ker} f = \text{im}(1 \to A) = 1$, so if $f(x) = 1$, $x = 1$, f injective.
If f injective, $\text{ker}f = 1$. $1 = \text{im}(1 \to A)$. $1 \to A \overset{f}{\mapsto} B$, exact.
(2) $\text{ker}(C \to 1) = C$, by def. of $C \to 1$
if $B \overset{g}{\mapsto} C \to 1$ exact, $\text{im}g = g(B) = \text{ker}(C \to 1) = C$. $g(B) = C$ implies g surjective.
If g surjective, $g(B) = C = \text{ker}(C \to 1)$. $B \overset{g}{\mapsto} C \to 1$ 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. □

2.1. 1st, 2nd, 3rd Isomorphism Theorems.

Theorem 9 (1st Isomorphism Theorem (Modules) Thm. 7.8 of Rotman (2010) [10])**.** *If $f : M \to N$ is R-map of modules, then $\exists$ R-isomorphism s.t.*

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

(5)
$$\varphi : M/kerf \to imf$$
$$\varphi : m + kerf \mapsto f(m)$$

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 $m + \text{ker}f = m' + \text{ker}f$, $m, m' \in M$, then $\exists n \in \text{ker}f$ s.t. $m = m' + n$.

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

$\Longrightarrow \varphi$ 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. $y = f(m)$. $f(m) = \varphi\pi(m) = \varphi(m + \text{ker}f) = y$. So $y \in \text{im}\varphi$. $\text{im}f \subseteq \text{im}\varphi$.
$\Longrightarrow \varphi$ surjective.
(φ injective) If $\varphi(a + \text{ker}f) = \varphi(b + \text{ker}f)$, then

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

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 10 (2nd Isomorphism Theorem (Modules) Thm. 7.9 of Rotman (2011) [10])**.** *If S, T are submodules of module M, i.e. $S, T \in M$, then $\exists$ $R-$isomorphism*

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

(6)
$$S/(S \cap T) \to (S + T)/T$$

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

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

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 11 (3rd Isomorphism Theorem (Modules) Thm. 7.10 of Rotman (2011) [10])**.** *If $T \subseteq S \subseteq M$ is a tower of submodules, then $\exists$ R-isomorphism*

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

(7)
$$(M/T)/(S/T) \to M/S$$

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

(8)
$$g : M + T \mapsto m + S$$

g well-defined: if $m + T = m' + T$, then $m - m' \in T \subseteq S$, and $m + S = m' + S \Longrightarrow g(m + T) = g(m' + T)$
$\text{ker}g = S/T$ since

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

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

$$g(m + T) = m + S \Longrightarrow \; \text{im}g \subseteq M/S$$
$$m + S = g(m + T)$$

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

3. Commutative Rings

cf. Ch. 3 "Commutative Rings I" of Rotman (2010) [10]

Definition 7. *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: $x + y = y + x$.

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

Proposition 5 (Matrix representation of linear transformation; 3.94 of Rotman (2010) [10])**.** *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 $\begin{array}{ll} (e_1 \dots e_n) & \text{standard basis of } k^n \\ (e_1' \dots e_m') & \text{standard basis of } k^m \end{array}$

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

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

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

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

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

□

4. R-modules

cf. Sec. 7.1 Modules of Rotman (2010) [10]

Definition 8 (R-module)**.** *R-module is (additive) abelian group M,*

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

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 $\begin{array}{l} i \in I \\ r \in R \end{array}$, 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 $A \in \text{Mat}_k(n,n)$, let linear $\begin{array}{l} T : k^n \to k^n. \\ T(w) = Aw \end{array}$

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 9 (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 [10]]

(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 $\varphi : V \to k^n$
$\varphi(v_i) = e_i$

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

$\implies \varphi(xv) = x\varphi(v) \quad \forall v \in V$
By induction on $\deg(f)$, $\varphi(f(x)v) = f(x)\varphi(v) \quad \forall f(x) \in k[x] \quad \forall v \in V$
$\implies \varphi$ is $k[x]$-map
$\implies \varphi$ is $k[x]$-isomorphism of V^T and $(k^n)^A$.

Proposition 6 (7.3 of Rotman (2011) [10]). *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) [10]). *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
$T : k^n \to k^n$
$T(y) = A(y)$ where $y \in k^n$ is a column.
By Example 7.1 (v) of Rotman (2011) [10], 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. 6,
$\exists$ isomorphism $\varphi : k^n \to k^n$ s.t. $B = \varphi A \varphi^{-1}$.
By Prop. 5, i.e. Prop. 3.94 of Rotman (2011) [10], in that every linear transformation has a matrix representation (even in the standard "Euclidean" basis), $\exists P \in \mathrm{Mat}_k(n,n)$, 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. 6,
$(k^n)^B$, $(k^n)^A$ are $k[x]$-isomorphic.
i.e. $\varphi : (k^n)^A \to (k^n)^B$ is a $k[x]$-module isomorphism.

□

Definition 10 ($\mathrm{Hom}_R(M,N)$).
(9)
$$Hom_R(M,N) = \{ \text{ all } R\text{-homomorphisms } M \to N \ \} = \{ f | f : M \to N, \text{ s.t. } \forall m, m' \in M, \forall r \in R, \begin{matrix} f(m+m') = f(m) + f(m') \\ f(rm) = rf(m) \end{matrix} \}$$

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

(10)
$$f + g : M \to N$$
$$f + g : m \mapsto f(m) + g(m)$$

Proposition 7 ($\mathrm{Hom}_R(M,N)$ R-module, 7.5 of Rotman (2011) [10]). *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. $\forall\, f, g \in \mathrm{Hom}_R(M,N)$, $\forall\, r, r', 1 \in R$,

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

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

□

Definition 11. *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 12 (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

$$\begin{aligned} \pi &: M \to M/N \\ m &\mapsto m + N \end{aligned} \tag{11}$$

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 8 (7.15 of Rotman (2010) [10])**.** (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.*

$$\begin{gathered} M = im(i) + im(j) \text{ and} \\ im(i) \bigcap im(j) = \{0\} \end{gathered} \tag{12}$$

(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*

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

s.t.

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

Proof.

- (i)$\to$ (ii) Given $S \bigsqcup T \simeq M$,
let $\varphi : S \bigsqcup T \to M$ be this isomorphism.
Define
$$\begin{aligned} i &:= \varphi\lambda_S & \quad (\lambda_S &: s \mapsto (s,0)) & \quad i &: S \to M \\ j &:= \varphi\lambda_T & \quad (\lambda_T &: t \mapsto (0,t)) & \quad j &: T \to M \end{aligned}$$
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
$$m = \varphi(s,t) = \varphi((s,0) + (0,t)) = \varphi\lambda_S(s)\varphi\lambda_T(t) = is + jt \in \mathrm{im}(i) + \mathrm{im}(j)$$
Let $c \in \mathrm{im}(i) + \mathrm{im}(j)$. Since $\begin{aligned} i &: S \to M \\ j &: T \to M \end{aligned}$, $c \in M$.
$\Longrightarrow M = \mathrm{im}(i) + \mathrm{im}(j)$.
If $x \in \mathrm{im}(i) \bigcap \mathrm{im}(j)$,
$$\begin{aligned} x &= i(s) \text{ for some } s \in S \\ x &= j(t) \text{ for some } t \in T \end{aligned}$$
$$is = jt = \varphi\lambda_S(s) = \varphi\lambda_T(t) = \varphi(s,0) = \varphi(0,t)$$
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. $M = \mathrm{im}(i) + \mathrm{im}(j)$, 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. $m = i(s'_+ j(t')$.
$$i(s - s') = j(t - t') \in \mathrm{im}(i) \bigcap \mathrm{im}(j) = \{0\}$$
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
$$\begin{aligned} p &: M \to S & \quad q &: M \to T \\ p(m) &:= s & \quad q(m) &:= t \end{aligned}$$
$$\begin{aligned} pi(s) &= s & \quad pj(t) &= 0 \\ qj(t) &= t & \quad qi(s) &= 0 \end{aligned} \qquad (ip + jq)(m) = ip(m) + jq(m) = i(s) + j(t) = m$$

□

5. Categories; Category Theory

5.1. Categories.

cf. 7.2 Categories of Rotman (2010) [10]

5.1.1. *Russell paradox, Russell set.*

Definition 13 (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 14 (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) $\exists \mathbf{1}, \forall f : A \to B, \exists \begin{array}{l} 1_A : A \to A \\ 1_B : B \to B \end{array}$ *, s.t.* $1_B \cdot f = f = f \cdot 1_A$*, and*

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

In summary,

$$\mathbf{C} := (Obj(\mathbf{C}), Mor\mathbf{C}, \circ, \mathbf{1}) \equiv (Obj\mathbf{C}, Mor\mathbf{C}, \circ_{\mathbf{C}}, \mathbf{1}_{\mathbf{C}}) \tag{13}$$

s.t.

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

Examples (7.25 of Rotman (2010)[10]):

(i) $\mathbf{C} =$ Sets
(ii) $\mathbf{C} =$ Groups = Grps
(iii) $\mathbf{C} =$ 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 15 (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.*

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

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 16 (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 $\begin{array}{ll} \alpha : A \to A', & \alpha : a \mapsto (a,1), \\ \beta : B \to B' & \beta : b \mapsto (b,2) \end{array}$ denote $A' \bigcup B' \equiv A \coprod B$.
From Rotman (2010) [10], pp. 447,

Definition 17. ***coproduct*** $A \coprod B \equiv C \in Obj(\mathcal{C})$

In my notation,
coproduct

$$\begin{gathered} (\mu_1, A_1 \coprod A_2) \\ (\mu_2, A_1 \coprod A_2) \end{gathered} \tag{14}$$

where injection (morphisms)

$$\begin{gathered} \mu_1 : A_1 \to A_1 \coprod A_2 \\ \mu_2 : A_1 \to A_1 \coprod A_2 \end{gathered} \tag{15}$$

s.t.

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

then

$$\begin{gathered} \exists ! [f_i] \equiv [f_1, f_2] \in \text{Mor}\mathbf{A},\ [f_1, f_2] : A_1 \coprod A_2 \to A \text{ s.t.} \\ [f_1, f_2]\mu_1 = f_1 \\ [f_1, f_2]\mu_2 = f_2 \end{gathered} \tag{16}$$

i.e.

$$\begin{tikzcd}
 & A \\
A_1 \arrow[ur, "f_1"] \arrow[r, "\mu_1"] & A_1 \coprod A_2 \arrow[u, dashed, "{[f_1, f_2]}"'] \\
A_2 \arrow[ur, "\mu_2"'] \arrow[uur, "f_2"]
\end{tikzcd} \tag{17}$$

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

$$\begin{gathered} \exists !\, [f_i] \equiv [f_i]_{i \in I} \in \text{Mor}\mathbf{A},\ [f_i] : \coprod_{i \in I} A_i \to A \text{ s.t.} \\ [f_i]\mu_j = f_j \qquad \forall\, j \in I \end{gathered} \tag{18}$$

i.e.

$$\begin{tikzcd}
 & A \\
A_j \arrow[ur, "f_j"] \arrow[r, "\mu_j"] & \coprod_{i \in I} A_i \arrow[u, dashed, "{[f_i]}"']
\end{tikzcd} \tag{19}$$

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 18 (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
$$f + g = g + f \qquad \textit{(additive abelian)}$$

5.1.2. *Examples of extra assumptions on sets,* ${}_R\boldsymbol{Mod}$ *we take for granted.* In Prop. 7.15(iii) Rotman (2010) [10],

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

$$ip + jq = 1_M$$

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 $\rho(s) = s$, $\forall\, s \in \text{im}\rho$.

$$S \xrightarrow{\ i\ } M \xleftarrow{\ j\ } T \qquad \text{and } M \simeq S \coprod T,$$

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.

$$\begin{aligned} i &: S \to M \\ p &: M \to S \end{aligned}$$

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

Definition 19 (free products)**.** ***free products*** *are coproducts in groups*

Prop. 7.26, Rotman (2010) [10]

Proposition 9 (7.26, Rotman)**.** *If* A, B *are* R*-modules,*
then their coproducts in ${}_R\boldsymbol{Mod}$ *exists, and it's the direct sum* $C = A \coprod B$.

Proof. Define

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

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

Define

$$\begin{aligned} \theta &: C \to X \\ \theta &: (a, b) \mapsto f(a) + g(b) \end{aligned}$$

$$\begin{aligned} \theta\mu(a) &= \theta(a, 0) = f(a) \\ \theta\nu(b) &= \theta(0, b) = g(b) \end{aligned}$$

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,

$$\begin{aligned}
\psi((a,0)) &= f(a) \qquad \forall\, a \in A \\
\psi((0,b)) &= g(b) \qquad \forall\, b \in B
\end{aligned}$$

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) [10]

Proposition 10 (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 $\begin{aligned} \mu_A &: A \to C, & \nu_A &: A \to D \\ \mu_B &: B \to C, & \nu_B &: B \to D \end{aligned}$

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

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. $\square$

Exer. 7.29 on pp. 459 of Rotman (2010) [10]

Definition 20. *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

$$\prod_i X_i := \varprojlim \alpha \qquad (20)$$

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

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

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 11 (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. □

5.1.3. *Products of Modules and Sets.*

Proposition 12 (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*

$$A \sqcap B \cong A \sqcup B \tag{21}$$

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

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

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

define $\begin{aligned} &\theta : X \to A \sqcup B \\ &\theta(x) = if(x) + jg(x) \end{aligned}$ 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 21. *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) [10]

Theorem 12 (7.32, Rotman)**.** *Let commutative ring R. $\forall$ R-module A, $\forall$ family $\{B_i | i \in I\}$ of R-modules,*

$$Hom_R(A, \prod_{i \in I} B_i) \simeq \prod_{i \in I} Hom_R(A, B_i) \tag{22}$$

via R-isomorphism

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

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

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

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

φ additive.

$\forall\, i, \forall\, r \in R$, $p_i r f = r p_i f$ (since product of R-modules, $\prod_{i \in I} B_i$ is also an R-module of $\mathrm{Obj}_R\mathbf{Mod}$, 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 $(f_i) \in \prod_i \mathrm{Hom}_R(A, B_i)$, then $f_i : A \to B_i \quad \forall\, i$

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

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

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

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 $p_i f = 0 \quad \forall\, i$

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

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

Part 2. Reading notes on Cox, Little, O'Shea's *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*

6. Geometry, Algebra, and Algorithms

6.1. Polynomials and Affine Space.

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

Definition 22 (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)

6.2. Affine Varieties.

6.3. Parametrizations of Affine Varieties.

6.4. Ideals.

6.5. Polynomials of One Variable.

7. Groebner Bases

7.1. Introduction.

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

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

7.4. Monomial Ideals and Dickson's Lemma.

7.5. The Hilbert Basis Theorem and Groebner Bases.

7.6. Properties of Groebner Bases.

7.7. Buchberger's Algorithm.

8. Elimination Theory

8.1. The Elimination and Extension Theorems.

8.2. The Geometry of Elimination.

9. The Algebra-Geometry Dictionary

9.1. Hilbert's Nullstellensatz.

9.2. Radical Ideals and the Ideal-Variety Correspondence.

10. Polynomial and Rational Functions on a Variety

10.1. Polynomial Mappings.

11. Robotics and Automatic Geometric Theorem Proving

11.1. Geometric Description of Robots.

Part 3. 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

12. Introduction

12.1. Polynomials and Ideals.

monomial

(23) $$(1.1) \qquad x_1^{\alpha_1} \dots x_n^{\alpha_n}$$

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

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

Done.

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

Definition 24 (1.5)**.** *Let $I\subset k[x_1\dots x_n]$, $I\neq\emptyset$*
I ideal if

(a) $f+g\in I$, $\forall f,g\in I$
(b) $pf\in I$, $\forall f\in I$, *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 $f\in\langle f_1\dots f_s\rangle$, $f=\sum_{i=1}^s p_i f_i$, $p_i\in k[x_1\dots x_n]$

$\forall i = 1\dots s$, $p_i f_i\in J$ 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 25 (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

12.2.

12.3. Gröbner Bases.

Definition 26 (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 $\text{LT}(I)$

12.4. **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 27 (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 $\mathbb{R}[x,y]$, $I = \{px^2 | p \in k[x,y]\}$
$I \subset I(V)$, since $px^2 = 0$ for $x^2 = 0$, $(0,b)$, $b \in \mathbb{R}$
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 $f \in \sqrt{I}$, $I \subset \sqrt{I}$
Hilbert basis thm., $\forall$ ideal $I \subset k[x_1 \dots x_n]$ s.t. $I = \langle f_1 \dots f_s \rangle$
$\underbrace{\quad}_{V(I) = \{(a_1 \dots a_n) | (a_1 \dots a_n) \in k^n,\, f_1(a_1 \dots a_n) = \dots = f_s(a_1 \dots a_n) = 0\}}$
$\mathbf{I}(\mathbf{V}(I)) = \{f \in k[x_1 \dots x_n] | f(a_1 \dots a_n) = 0 \quad \forall (a_1 \dots a_n) \in V(I)\}$
Let $g \in \sqrt{I}$, $g^m \in I$, $g^m = g^{m-1} g$
$g^m(a_1 \dots a_n) = 0 = g^{m-1}(a_1 \dots a_n) g(a_1 \dots a_n) = 0$. 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.

13. Solving Polynomial Equations

13.1.

13.2. **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, $\forall f \in I$, $\text{LT}(f)$ divisible by $\text{LT}(g_i)$ 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 $\text{LT}(I)$ 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

$$f = h_1 g_1 + \dots + h_t g_t + \overline{f}^G \qquad (2.1) \qquad (24)$$

where remainder $\overline{f}^G$ is a linear combination of monomials $x^\alpha \notin \langle \text{LT}(I) \rangle$
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

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

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

13.3.

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

14. Resultants

15. Computation in Local Rings

15.1. **Local Rings.**

Definition 28 (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 13 (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 $g_1(p) \neq 0$, $g_2(p) \neq 0$

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

$f = \frac{f}{I} \in R$, $\forall f \in k[x_1 \dots x_n]$, 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 $k(x_1 \dots x_n)$ $\quad k(x_1 \dots x_n) \subset R$

(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 29 (1.3)**.** *local ring is a ring that has exactly 1 maximal ideal*

Proposition 14 (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.

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

$k[t]_{\langle t \rangle}$ $\quad \frac{-2t^2}{1+t^2}$ 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

$$k\{x_1 \dots x_n\} = \{ \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha | c_\alpha \in k, \text{ series converges in some open } U \ni 0 \in k^n \, \} \tag{25} \quad (1.5)$$

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

$$k[[x_1 \dots x_n]] = \{ \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha | c_\alpha \in k \} \text{ series need not converge} \tag{26} \quad (1.6)$$

variety V

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

15.2. **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 30 (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*

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

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

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

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

16.

17.

18. Polytopes, Resultants, and Equations

19. Polyhedral Regions and Polynomials

19.1. **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?

$$\begin{aligned} 4A + 5B &\leq 37 \\ 2A + 3B &\leq 20 \\ A, B &\in \mathbb{Z}^*_{\geq 0} \end{aligned} \tag{27} \quad (1.1)$$

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"

$$a_{ij} A_j = b_i, \quad A_j \in \mathbb{Z}_{\geq 0} \tag{28} \quad (1.4)$$

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 15 (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 16 (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.

19.2. Integer Programming and Combinatorics.

20. Algebraic Coding Theory

21. The Berlekamp-Massey-Sakata Decoding Algorithm

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

Part 4. Statistical Mechanics: Ising Model

22. Ising Model

22.1. 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.

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

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. $(i, j) \in \mathbb{Z}^2$. $\begin{array}{l} i \in 0, 1, \dots L_x - 1 \\ j \in 0, 1, \dots L_y - 1 \end{array}$. 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 $\mathbf{k} \mapsto (i, j), (i \pm 1, j), (i, j \pm 1)$, $\begin{array}{l} i = 1 \dots L_x - 2 \\ j = 1 \dots L_y - 2 \end{array}$.

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"

22.1.1. *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 $\sigma : \Lambda \mapsto (\sigma_{\mathbf{k}})_{\mathbf{k}\in\Lambda} \in \{-1, 1\}^{|\Lambda|}$.

$$H(\sigma) = -\sum_{\langle ij \rangle} J_{ij} \sigma_i \sigma_j - \mu \sum_j h_j \sigma_j \equiv H(\sigma(\Lambda)) = -\sum_{\langle \mathbf{kl} \rangle} J_{\mathbf{kl}} \sigma_{\mathbf{k}} \sigma_{\mathbf{l}} - \mu \sum_{\mathbf{k}\in\Lambda} h_{\mathbf{k}} \sigma_{\mathbf{k}} \tag{29}$$

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 [5]

EY : 20171223 Things to check from Hjorth-Jensen (2015) [6]:

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

$$P_\beta(\sigma) = \frac{\exp(-\beta H(\sigma))}{Z_\beta} = \text{ prob. of configuration } \sigma \equiv \sigma(\Lambda) \equiv (\sigma_{\mathbf{k}})_{\mathbf{k}\in\Lambda} \tag{30}$$

with the partition function as normalization constant Z_β:

$$Z_\beta = \sum_\sigma \exp -\beta H(\sigma) \tag{31}$$

cf. pp. 504 Sec. 151 Phase transitions of the second kind in a 2-dim. lattice, Landau and Lifshitz [5]

$$Z = 2^N (1-x^2)^{-N} \prod_{p,q=0}^{L-1} \left[(1+x^2)^2 - 2x(1-x^2)\left(\cos\frac{2\pi p}{L} + \cos\frac{2\pi q}{L} \right) \right]^{1/2} \tag{32}$$

cf. (151.11) of Landau and Lifshitz [5], where $x = \tanh\theta$, $\theta = J/T \equiv J/\tau = \beta J$.

$$\begin{aligned} \Phi \equiv F = -\tau \ln Z = & \\ = -\tau N \ln 2 + \tau N \ln(1-x^2) - \frac{\tau}{2} \sum_{p,q=0}^{L} \ln & \left[(1+x^2)^2 - 2x(1-x^2)\left(\cos\frac{2\pi p}{L} + \cos\frac{2\pi q}{L} \right) \right] \end{aligned} \tag{33}$$

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 $-1 < x < 1$)

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

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

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

$$\boxed{\tau_c = \frac{2J}{\ln(1+\sqrt{2})}} \tag{34}$$

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

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

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

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

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 [5], L.Onsager 1947.

22.2. **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) [7] 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) [7].

However, none of these promised simple calculations were shown explicitly in Newman and Barkema (1999) [7]. I will forego this simple case.

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

$$H(\sigma) = -\sum_{\langle \mathbf{kl} \rangle} J\sigma_{\mathbf{k}}\sigma_{\mathbf{l}} = -J\sum_{i=0}^{L_x-1}\sum_{j=0}^{L_y-1}\sigma_{ij}(\sigma_{i+1j} + \sigma_{ij+1}) =$$

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

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

Now for each of these terms,

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

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

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

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

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:

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

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

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

$$(35)\quad = \frac{-J}{2}\left[\sum_{i=0}^{L_x-1}\left(\sum_{\substack{j=0\\ j\neq j'}}^{L_y-1}\sigma_{ij}(\sigma_{i+1j}+\sigma_{i-1j}+\sigma_{ij+1}+\sigma_{ij-1}) + \sigma_{ij'}(\sigma_{i+1j'}+\sigma_{i-1j'}+\sigma_{ij'+1}+\sigma_{ij'-1})\right) + \right.$$
$$\left. \sum_{\substack{j=0\\ j\neq j'}}^{L_y-1}\sigma_{i'j}(\sigma_{i'+1j}+\sigma_{i'-1j}+\sigma_{i'j+1}+\sigma_{i'j-1}) + \sigma_{i'j'}(\sigma_{i'+1j'}+\sigma_{i'-1j'}+\sigma_{i'j'+1}+\sigma_{i'j'-1})\right]$$

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

$$(36)\quad \Delta H(\Delta\sigma_{i'j'}) = 2J\sigma_{i'j'}(\sigma_{i'+1j'}+\sigma_{i'-1j'}+\sigma_{i'j'+1}+\sigma_{i'j'-1})$$

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 5. Conformal Field Theory; Virasoro Algebra

cf. Schottenloher (2008) [4]

23. Conformal Transformations

Definition 32 (Conformal transformation or conformal map)**.** *Let 2 semi-Riemannian manifolds(M,g), (M',g'), $dimM = dimM'$, 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.*

$$(37)\quad \varphi^*g' = \Omega^2 g$$

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 33. ***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) [4].

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. $a\in A, b\in E \Longrightarrow i(a)b = bi(a)$.

23.0.1. *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
$$\begin{aligned} i : A &\to A\times G \\ a &\mapsto (a,1) \end{aligned}$$

$$\begin{gathered} i(a)(a',g) = (a,1)(a',g) = (aa',g) = \\ = (a'a, g\cdot 1) = (a',g)(a,1) = (a',g)i(a) \end{gathered}$$

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

(38)
$$1 \longrightarrow \mathbb{Z}/k\mathbb{Z} \longrightarrow E\times U(1) \xrightarrow{\pi} U(1) \longrightarrow 1$$

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 34 (semi-direct product)**.** ***semidirect product*** *group $G\ltimes H$ is set $H\times G$, with multiplication*
$$(x,g)\cdot(x',g') := (x\tau(g)(x'), gg') \qquad \forall\,(x,g),(x',g')\in H\times G$$

(39)
$$1 \longrightarrow H \xrightarrow{i} G\ltimes H \xrightarrow{\pi} G \longrightarrow 1$$

with

(40)
$$\begin{aligned} i &: H \to G\ltimes H \\ i(x) &= (x,1) \end{aligned}$$

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

(41)
$$\begin{aligned} \pi &: G\ltimes H \to G \\ \pi(x,g) &= g \end{aligned}$$

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 35 (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. 34 and Def. 35 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. $H\triangleleft G$,
$$\begin{gathered} (x,g)(h,1)(\tau(g^{-1})x^{-1}\tau(g^{-1}), g^{-1}) = (x\tau(g)h, g)(\tau(g^{-1})x^{-1}\tau(g^{-1}),g^{-1}) = \\ = (x\tau(g)h\tau(g)\tau(g^{-1})x^{-1}\tau(g^{-1}),1) = (x\tau(g)hx^{-1}\tau(g^{-1}),1) \end{gathered}$$

$\Longrightarrow$ H normal subgroup of $G\ltimes H \equiv H\triangleleft(G\ltimes H)$.
Notes on Semidirect products

- extension

$$1 \longrightarrow SL(n,\mathbb{R}) \xrightarrow{i} GL(n,\mathbb{R}) \xrightarrow{\det} \mathbb{R}^* \longrightarrow 1 \tag{42}$$

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

$$\mathbb{R}^* \simeq \{a 1_n | a \in \mathbb{R}^*\}$$

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. 35, 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 6. Algebraic Topology

cf. Bredon (1997) [8]

24. Simplicial Complexes

cf. pp. 245, from Sec. 21 Simplicial Complexes of Ch. 4 Homology Theory in Bredon (1997) [8]
$\mathbf{v}_0, \dots \mathbf{v}_n \in \mathbb{R}^\infty$, "affinely independent" if they span an affine n-plane, i.e.

$$\text{if } \left(\sum_{i=0}^n \lambda_i \mathbf{v}_i = 0, \sum_{i=0}^n \lambda_i = 0 \right), \text{ then } \implies \forall \, \lambda_i = 0$$

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

$$\sigma = (\mathbf{v}_0, \dots \mathbf{v}_n) = \{\sum_{i=0}^n \lambda_i \mathbf{v}_i | \sum_{i=0}^n \lambda_i = 1, \, \lambda_i \geq 0\} \tag{43}$$

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 36. *(geometric) simplicial complex $K :=$ collection of affine simplices s.t.*
(1) *$\sigma \in K \implies$ any face of $\sigma \in K$; and*
(2) *$\sigma, \tau \in K \implies \sigma \bigcap \tau$ 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 37 (Def. 21.2 of Bredon (1997) [8])**.** *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) [8].
Then this gives CW-complex structure on $|K|$ with f_σ as characteristic maps.

Part 7. Graphs, Finite Graphs

25. Graphs, Finite Graphs, Trees

Serre (1980) [9]
cf. Chapter I. Trees and Amalgams, Section 1 Amalgams, Subsection 1.1 Direct limits of Serre (1980) [9]
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 17. *$\exists !$ 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 $H \mapsto \varinjlim \text{Hom}(G_i, H)$.
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

$$\pi_1(U_{12}; x) \to \pi_1(U_1; x)$$
$$\pi_1(U_{12}; x) \to \pi_1(U_2; x)$$

Exercise 1. Let homomorphisms $f_1 : A \to G_1$ amalgam $G = G_1 *_A G_2$.
$f_2 : A \to G_2$
Define subgroups A^n, G_1^n, G_2^n, of A, G_1, G_2 recursively by

$$A^1 = \{1\}$$
$$G_1^1 = \{1\}$$
$$G_2^1 = \{1\}$$

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).

$$A^2 = \langle f_1^{-1}(G_1^1), f_2^{-1}(G_2^1) \rangle = \langle f_1^{-1}(\{1\}), f_2^{-1}(\{1\}) \rangle$$
$$G_i^2 = f_i(A^2)$$

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

$$f_i(a) = f_i(a)G_i^\infty = f_i(a)f_i(A^{n_a}) = f_i(aA^{n_a})$$
$$f_i(b) = f_i(b)G_i^\infty = f_i(b)f_i(A^{n_b}) = f_i(bA^{n_b})$$

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) [9]
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.

25.0.1. *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.

$$i_m \neq i_{m+1} \text{ for } 1 \leq m \leq n-1 \tag{44}$$

cf. (T) of Serre (1980) [9].
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, $f_1 : A \to G_1$.
$f_2 : A \to G_2$

$$G_1 \backslash f_1(A) = \{f_1(A)g | g \in G_1\}$$
$$G_2 \backslash f_2(A) = \{f_2(A)g | g \in G_2\}$$

$\mathbf{i} = (i_1 \dots i_n)$, $i_j \in I$, $i_m \neq i_{m+1}$ 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 38 (reduced word)**.** ***reduced word*** *of type* $\mathbf{i}$, m,

$$m = (a; s_1 \dots s_n) \tag{45}$$

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 13 (1 of Serre (1980) [9])**.** $\forall g \in G$, $\exists$ *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

$$\begin{aligned} &S_i = \{ g | g \in f_i(A) g \in f_i(A) G_i \} \\ &A \times S_i \to G_i \text{ onto} \\ &A \times (S_i - \{1\}) \to G_i - A \text{ onto} \\ &(a, s) \mapsto as \text{ bijection} \end{aligned}$$

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) [9]

Definition 39 (1. of Serre (1980) [9])**.** ***graph*** $\Gamma = (X, Y, Y \to X \times X, Y \to Y)$, *where* $\begin{aligned} \textit{set } X &= \textit{vert}\,\Gamma \\ \textit{set } Y &= \textit{edge}\,\Gamma \end{aligned}$

$$\begin{aligned} &Y \to X \times X \\ &y \mapsto (o(y), t(y)) \\ &Y \to Y \\ &y \mapsto \overline{y} \end{aligned}$$

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_+

25.0.2. *Realization of a Graph.* cf. Realization of a Graph in Serre (1980) [9].

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

$$\begin{aligned} (y, t) &\equiv (\overline{y}, 1 - t) \\ (y, 0) &\equiv o(y) \qquad \forall\, y \in Y, \forall\, t \in [0,1] \\ (y, 1) &\equiv t(y) \end{aligned} \tag{46}$$

quotient space $\text{real}(\Gamma) = T/R$ 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 40. *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 41 (connected graph; Def. 3 of Serre (1980) [9])**.** *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.*

25.0.3. *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 42 (circuit; Def. 4 of Serre (1980) [9])**.** *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 $\in \text{Circ}_1$.
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), $(1 \leq i \leq 2)$, $P_1 = t(y_1)$

$$P_2 = t(y_2) = o(y_1)$$

25.1. **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 43 (combinatorial; Def. 5 of Serre (1980) [9]). *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 8. Tensors, Tensor networks; Singular Value Decomposition, QR decomposition, Density Matrix Renormalization Group (DMRG), Matrix Product states (MPS)

26. 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) [13]).

26.1. **List of stuff I want to look at/do/study.** I would like to compare/contrast the following:

- Rotman (2010) [10], Ch. 8, but starting from 8.4 Tensor Products, pp. 574
- Jeffrey Lee (2009) [12], Ch. 7 Tensors

Maldacena and Susskind (2013) [17]
Lectures on Gravity and Entanglement. Mark Van Raamsdonk [20]

- Consider as physical system AdS-Schwarzchild black hole
- CFT
  - PFL Lectures on Conformal Field Theory in $D \geq 3$ Dimensions, Rychkov (2016) [18].

Evenbly and Vidal (2011) [19], 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

26.2. **Tensor operations; Tensor properties.**

26.2.1. *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

$$[A \otimes B]_{i_1 \dots i_r, j_1 \dots j_s} := A_{i_1 \dots i_r} \cdot B_{j_1 \dots j_s} \tag{47}$$

26.2.2. *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

$$[\mathrm{Tr}_{x,y} A]_{i_1 \dots i_{x-1} i_{x+1} \dots i_{y-1} i_{y+1} \dots i_r} = \sum_{\alpha=1}^{d_x} A_{i_1 \dots i_{x-1} \alpha i_{x+1} \dots i_{y-1} \alpha i_{y+1} \dots i_r} \tag{48}$$

26.2.3. *Contraction.*

26.2.4. *Group and splitting, Bridgeman and Chubb (2017)* [13]. "Rank is a rather fluid concept in the study of tensor networks." Bridgeman and Chubb (2017) [13].

$\mathbb{C}^{a_1 \times \dots \times a_n} \simeq \mathbb{C}^{b_1 \times \dots \times b_m}$ 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) [13]; check this)

"Owing to freedom in choice of basis, precise details of grouping and splitting aren't unique." (cf. Bridgeman and Chubb (2017) [13]).

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."

$$|0\rangle \otimes |1\rangle \equiv |0\rangle \tag{49}$$

and precisely this grouping,

$$\begin{gathered} |0\rangle \otimes |1\rangle \in \mathrm{Mat}_{\mathbb{C}}(2,2), \text{ whilst} \\ |01\rangle \in \mathbb{C}^4 \end{gathered} \tag{50}$$

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):

$$\begin{gathered} \mathbb{K}^{d_1^{(i)}} \times \mathbb{K}^{d_2^{(i)}} \times \dots \times \mathbb{K}^{d_n^{(i)}} \times \mathbb{K}^{d_1^{(j)}} \times \mathbb{K}^{d_2^{(j)}} \times \dots \times \mathbb{K}^{d_m^{(j)}} \xrightarrow{\text{flatten}} \mathbb{K}^{\prod_{p=1}^n d_p^{(i)}} \times \mathbb{K}^{\prod_{q=1}^m d_q^{(j)}} \\ T_{i_1 \dots i_n, j_1 \dots j_m} \xmapsto{\text{flatten}} T_{I,J} \\ \{0,1,\dots d_1^{(i)}\} \times \{0,1,\dots d_2^{(i)}\} \times \dots \times \{0,1,\dots d_n^{(i)}\} \times \{0,1,\dots d_1^{(j)}\} \times \{0,1,\dots d_2^{(j)}\} \times \dots \times \{0,1,\dots d_m^{(j)}\} \xrightarrow{\text{flatten}} \\ \xrightarrow{\text{flatten}} \{0,1,\dots \prod_{p=1}^n d_p^{(i)} - 1\} \times \{0,1,\dots \prod_{q=1}^m d_q^{(j)} - 1\} \\ (i_1, i_2, \dots i_n, j_1, j_2 \dots j_m) \xmapsto{\text{flatten}} (I,J) := (i_1 + d_1^{(i)} i_2 + \dots + d_1^{(i)} \dots d_{n-1}^{(i)} i_n, j_1 + d_1^{(j)} j_2 + \dots + d_1^{(j)} \dots d_{m-1}^{(j)} j_m) \end{gathered} \tag{51}$$

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 $J = 0$).

26.3. Singular Value Decomposition.

$$T_{I,J} = \sum_\alpha U_{I,\alpha} S_{\alpha,\alpha} \overline{V}_{J,\alpha}$$

$$\begin{gathered} \mathrm{Mat}_{\mathbb{K}}(N,M) \xrightarrow{\text{SVD}} \mathrm{Mat}_{\mathbb{K}}(N,P) \times \mathrm{Mat}_{\mathbb{K}}(P,P) \times \mathrm{Mat}_{\mathbb{K}}(M,P) \\ T_{I,J} \xmapsto{\text{SVD}} U_{I,\alpha}, S_{\alpha,\alpha}, \overline{V}_{I,\alpha} \text{ s.t.} \\ T_{I,J} = \sum_\alpha U_{I,\alpha} S_{\alpha,\alpha} \overline{V}_{J,\alpha} \\ T = USV^\dagger \end{gathered} \tag{52}$$

For the higher-dimensional version of SVD,

$$\begin{gathered} \mathbb{K}^{d_1^{(i)}} \otimes \dots \otimes \mathbb{K}^{d_N^{(i)}} \otimes \mathbb{K}^{d_1^{(j)}} \otimes \dots \otimes \mathbb{K}^{d_M^{(j)}} \xrightarrow{\text{flatten}} \mathrm{Mat}_{\mathbb{K}}(N,M) \xrightarrow{\text{SVD}} \mathrm{Mat}_{\mathbb{K}}(N,P) \times \mathrm{Mat}_{\mathbb{K}}(P,P) \times \mathrm{Mat}_{\mathbb{K}}(M,P) \xrightarrow{\text{splitting}} \\ \xrightarrow{\text{splitting}} \mathbb{K}^{d_1^{(i)}} \otimes \dots \otimes \mathbb{K}^{d_N^{(i)}} \otimes \mathbb{K}^P \times \mathrm{Mat}_{\mathbb{K}}(P,P) \times \mathbb{K}^{d_1^{(j)}} \otimes \dots \otimes \mathbb{K}^{d_M^{(j)}} \otimes \mathbb{K}^P \\ T_{i_1 \dots i_N, j_1 \dots j_M} = \sum_\alpha U_{i_1 \dots i_N, \alpha} S_{\alpha,\alpha} \overline{V}_{j_1 \dots j_M, \alpha} \end{gathered} \tag{53}$$

27. Density Matrix Renormalization Group; Matrix Product States (MPS)

cf. Sec. 4, Matrix Product States (MPS) of Schollwöck [15].

Necessarily, given matrix $M \in \mathrm{Mat}_{\mathbb{K}}(M,N)$ (notation in Bridgeman and Chubb (2017) [13] and CUDA Toolkit Documentation; I will follow the notation in Schollwöck [15] since his A,B denote specific physical meaning).

For

$$\begin{gathered} U \in \mathrm{Mat}_{\mathbb{K}}(N_A, \min(N_A, N_B)) \text{ s.t. } UU^\dagger = 1 \\ S \in \mathrm{Mat}_{\mathbb{K}}(\min(N_A, N_B), \min(N_A, N_B)) \end{gathered}$$

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 $s_1 \geq s_2 \geq \dots \geq s_r \geq 0$.
$V^\dagger \in \text{Mat}_{\mathbb{K}}(\min(N_A,N_B), N_B)$ s.t. $V^\dagger V = 1$.

$$\text{Mat}_{\mathbb{K}}(N_A,N_B) \xrightarrow{\text{SVD}} U_{\mathbb{K}}(N_A, \min(N_A,N_B)) \times \text{diag}_{\mathbb{K}}(\min(N_A,N_B)) \times U_{\mathbb{K}}(\min(N_A,N_B), N_B)$$

$$M \xmapsto{\quad\quad\quad\quad\text{SVD}\quad\quad\quad\quad} USV^\dagger$$

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 $\langle M|N\rangle = \text{tr}M^\dagger N$. Indeed,

$$\text{tr}M^\dagger N = (M^\dagger)_{ik}N_{ki} = \overline{M}_{ki}N_{ki}$$

and so for

$$M' = US'V^\dagger, \quad S' = \text{diag}(s_1, s_2 \dots s_{r'}, 0\dots) \tag{54}$$

cf. Eq. (19) of Schollwöck [15], 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

$$\widehat{\rho}_A = \text{tr}_B|\psi\rangle\langle\psi|$$
$$\widehat{\rho}_B = \text{tr}_A|\psi\rangle\langle\psi|$$

In matrix form,

$$\rho_A = \Psi\Psi^\dagger$$
$$\rho_B = \Psi^\dagger\Psi$$

Indeed,

$$(\rho_A)_{ij} = \Psi_{ik}\overline{\Psi}_{jk}$$
$$(\rho_B)_{ij} = \overline{\Psi}_{ki}\Psi_{kj}$$
$$|\psi\rangle\langle\psi| = \sum_{i,j}\Psi_{ij}|i\rangle_A|j\rangle_B \sum_{l,m}\overline{\Psi}_{lm}\langle l|_A\langle m|_B$$
$$\text{tr}_B|\psi\rangle\langle\psi| = \sum_{i,j}\Psi_{ik}\overline{\Psi}_{jk}|i\rangle_A\rangle j|_A$$

In matrix form,

$$\rho_A = \Psi\Psi^\dagger$$
$$\rho_B = \Psi^\dagger\Psi$$

Carry out SVD on Ψ in Eq. (20) of Schollwöck [15],

$$|\psi\rangle = \sum_{i,j}\Psi_{ij}|i\rangle_A|j\rangle_B$$

$$|\psi\rangle = \sum_{ij}\Psi_{ij}|i\rangle_A|j\rangle_B = \sum_{ij}\sum_{a=1}^{\min(N_A,N_B)} U_{ia}S_{aa}\overline{V}_{ja}|i\rangle_A|j\rangle_B = \sum_{a=1}^{\min(N_A,N_B)}\sum_i U_{ia}|i\rangle_A s_a \sum_j \overline{V}_{ja}|j\rangle_B = \sum_{a=1}^{\min(N_A,N_B)} s_a|a\rangle_A|a\rangle_B$$

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:

$$\widehat{\rho}_A = \sum_{a=1}^r s_a^2|a\rangle_A\langle a|_A$$
$$\widehat{\rho}_B = \sum_{a=1}^r s_a^2|a\rangle_B\langle a|_B$$

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

$$|\overline{\Psi}\rangle = \sum_{a=1}^{r'} s_a|a\rangle_A|a\rangle_B \tag{55}$$

cf. Eq. (27) of Schollwöck [15], where s_a must be rescaled if normalization desired.

27.1. **QR decomposition.** cf. 4.1.2. of Schollwöck [15].
If actual value of singular values not used explicitly, then use *QR decomposition.*
QR decomposition: $\forall\, M \in \text{Mat}_{\mathbb{K}}(N_A,N_B)$,

$$M = QR,\ Q \in U_{\mathbb{K}}(N_A),\ \text{i.e. } Q^\dagger Q = 1 = QQ^\dagger,\ R \in \text{Mat}_{\mathbb{K}}(N_A,N_B) \text{ s.t. upper triangular, i.e. } R_{ij} = 0 \text{ if } i > j \tag{56}$$

thin QR decomposition: assume $N_A > N_B$. Then bottom $N_A - N_B$ rows of R are 0, so

$$M = Q\begin{bmatrix} R_1 \\ 0 \end{bmatrix} = \begin{bmatrix} Q_1 & Q_2 \end{bmatrix}\begin{bmatrix} R_1 \\ 0 \end{bmatrix} = Q_1R_1$$
$$Q_1 \in \text{Mat}_{\mathbb{K}}(N_A,N_B)$$
$$R_1 \in \text{Mat}_{\mathbb{K}}(N_B,N_B)$$

While $Q_1^\dagger Q_1 = 1$ in general $Q_1Q_1^\dagger \neq 1$

28. Matrix Product States (MPS)

cf. Section 4.13 Decomposition of arbitrary quantum states into MPS of Schollwöck [15].
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)

$$|\psi\rangle = \sum_{\sigma_1\dots\sigma_L} c_{\sigma_1\dots\sigma_L}|\sigma_1\dots\sigma_L\rangle \tag{57}$$

cf. Eq. (30) of Schollwöck [15],

28.1. **Left-canonical matrix product state.** cf. Schollwöck [15],
Consider the process of refactoring or "flattening", which I claim to be a functor *flatten*:

$$|\psi\rangle \in \mathcal{H} \text{ s.t. } \dim\mathcal{H} = d^L \mapsto \Psi \in \mathrm{Mat}_{\mathbb{K}}(d, d^{L-1})$$

$$\Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} = c_{\sigma_1\dots\sigma_L}$$

$$\xrightarrow{\text{SVD}} c_{\sigma_1\dots\sigma_L} = \Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} = \sum_a^{r_1} U_{\sigma_1,a_1}S_{a_1,a_1}(V^\dagger)_{a_1,(\sigma_2\dots\sigma_L)} \equiv \sum_{a_1}^{r_1} U_{\sigma_1,a_1}c_{a_1,\sigma_2\dots\sigma_L} \tag{58}$$

i.e.

$$\begin{gathered}(\mathbb{K}^d)^L \to \mathrm{Mat}_{\mathbb{K}}(1,r)\times \mathrm{Mat}_{\mathbb{K}}(r_1 d, d^{L-2}) \\ c_{\sigma_1\dots\sigma_L} \mapsto A^{\sigma_1}_{a_1}, \Psi_{(a_1\sigma_2),(\sigma_3\dots\sigma_L)}\end{gathered}$$

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 [15],

$$c_{\sigma_1\dots\sigma_L} = \sum_{a_1}^{r_1}\sum_{a_2}^{r_2} A^{\sigma_1}_{a_1}U_{(a_1\sigma_2),a_2}S_{a_2,a_2}(V^\dagger)_{a_2,(\sigma_3\dots\sigma_L)} = \sum_{a_1}^{r_1}\sum_{a_2}^{r_2} A^{\sigma_1}_{a_1}A^{\sigma_2}_{a_1,a_2}\Psi_{(a_2\sigma_3),(\sigma_4\dots\sigma_L)} \tag{59}$$

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)

$$\xrightarrow{\text{SVD}} c_{\sigma_1\dots\sigma_L} = \sum_{a_1\dots a_{L-1}} A^{\sigma_1}_{a_1}A^{\sigma_2}_{a_1a_2}\dots A^{\sigma_{L-1}}_{a_{L-2},a_{L-1}}A^{\sigma_L}_{a_L-1} \equiv A^{\sigma_1}A^{\sigma_2}\dots A^{\sigma_{L-1}}A^{\sigma_L}$$

28.1.1. *Matrix Product State (definition).*

Definition 44 (Matrix Product State)**.**

$$|\psi\rangle = \sum_{\sigma_1\dots\sigma_L} A^{\sigma_1}A^{\sigma_2}\dots A^{\sigma_{L-1}}A^{\sigma_L}|\sigma_1\dots\sigma_L\rangle \tag{60}$$

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

$$\sum_{\sigma_l}(A^{\sigma_l})^\dagger A^{\sigma_l} = 1 \tag{61}$$

cf. Eq. (38) of Schollwöck [15],
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.

$$\begin{aligned}|a_l\rangle_A &= \sum_{\sigma_1\dots\sigma_l}(A^{\sigma_1}A^{\sigma_2}\dots A^{\sigma_l})_{a_l,1}|\sigma_1\dots\sigma_l\rangle \\ |a_l\rangle_B &= \sum_{\sigma_{l+1}\dots\sigma_L}(A^{\sigma_{l+1}}A^{\sigma_{l+2}}\dots A^{\sigma_L})_{a_l,1}|\sigma_{l+1}\dots\sigma_L\rangle\end{aligned}$$

s.t. matrix product state (MPS) is

$$|\psi\rangle = \sum_{a_l}|a_l\rangle_A|a_l\rangle_B$$

28.1.2. *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

$$(\mathbb{K}^d)^L \xrightarrow{\text{SVD}} (\mathrm{Mat}_{\mathbb{K}}(1,r_1))^d\times(\mathrm{Mat}_{\mathbb{K}}(r_1,r_2))^d\times\dots\times(\mathrm{Mat}_{\mathbb{K}}(r_{L-2},r_{L-1}))^d\times(\mathrm{Mat}_{\mathbb{K}}(r_{L-1},1))^d$$

$$c_{\sigma_1\dots\sigma_L} \xmapsto{\qquad\text{SVD}\qquad} c_{\sigma_1\dots\sigma_L} = \textstyle\sum_{a_1\dots a_{L-1}} A^{\sigma_1}_{a_1}A^{\sigma_2}_{a_1a_2}\dots A^{\sigma_{L-1}}_{a_{L-2},a_{L-1}}A^{\sigma_L}_{a_{L-1}}$$

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:

$$(\mathbb{K}^d)^L \xrightarrow{\text{flatten}^{-1}} \text{Mat}_{\mathbb{K}}(d,d^{L-1}) \xrightarrow{\text{SVD}} U_{\mathbb{K}}(d,r_1)\times \text{diag}_{\mathbb{K}}(r_1)\times U_{\mathbb{K}}(r_1,d^{L-1}) \xrightarrow{\cong} (\text{Mat}_{\mathbb{K}}(1,r_1))^d \times \text{Mat}_{\mathbb{K}}(r_1 d, d^{L-2}) \xrightarrow{\text{flatten}} (\text{Mat}_{\mathbb{K}}(1,r_1))^d\times(\mathbb{K}^{r_1})\times(\mathbb{K}^d)^{L-1}$$

$$c_{\sigma_1\dots\sigma_L} \xmapsto{\text{flatten}^{-1}} c_{\sigma_1\dots\sigma_L} = \Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} \xmapsto{\text{SVD}} \Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} = \sum_{a_1}^{r_1} U_{\sigma_1 a_1} S_{a_1,a_1}(V^\dagger)_{a_1,(\sigma_2\dots\sigma_L)} \xmapsto{\cong} c_{a_1\sigma_2\dots\sigma_L} = \sum_{a_1}^{r_1} A^{\sigma_1}_{a_1}\Psi_{(a_1,a_2),(\sigma_3\dots\sigma_L)} \xmapsto{\text{flatten}} c_{a_1\sigma_2\dots\sigma_L} = \sum_{a_1}^{r_1} A^{\sigma_1}_{a_1} c_{a_1\sigma_2\dots\sigma_L}$$

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:

$$\begin{gathered}(\mathbb{K}^d)^L \longrightarrow (\text{Mat}_{\mathbb{K}}(1,r_1))^d \times \mathbb{K}^{r_1}\times(\mathbb{K}^d)^{L-1} \\ c_{\sigma_1\dots\sigma_L} \longmapsto c_{\sigma_1\dots\sigma_L} = \sum_{a_1}^{r_1} A^{\sigma_1}_{a_1} c_{a_1\sigma_2\dots\sigma_L}\end{gathered}$$

So in summary, to obtain matrix product states, starting from a matrix,

$$\boxed{\begin{gathered}\text{Mat}_{\mathbb{K}}(d,d^{L-1}) \longrightarrow (\text{Mat}_{\mathbb{K}}(1,r_1))^d \times \text{Mat}_{\mathbb{K}}(r_1 d, d^{L-2}) \longrightarrow \dots \longrightarrow (\text{Mat}_{\mathbb{K}}(1,r_1))^d\times(\text{Mat}_{\mathbb{K}}(r_1,r_2))^d\times\dots\times(\text{Mat}_{\mathbb{K}}(r_{n-1},r_n))^d\times(\text{Mat}_{\mathbb{K}}(r_n d, d^{L-(n+1)}))^d \\ \Psi_{\sigma_1,(\sigma_2\dots\sigma_L)} \longmapsto \sum_{a_1}^{r_1} A^{\sigma_1}_{a_1}\Psi_{(a_1,a_2),(\sigma_3\dots\sigma_L)} \longmapsto \dots \longmapsto \sum_{a_1,a_2,\dots a_n}^{r_1,r_2,\dots r_n} A^{\sigma_1}_{a_1}A^{\sigma_2}_{a_1 a_2}\dots A^{\sigma_n}_{a_{n-1}a_n}\Psi_{(a_n\sigma_{n+1}),(\sigma_{n+2}\dots\sigma_L)}\end{gathered}} \tag{62}$$

28.2. **Right-canonical matrix product state.** cf. Schollwöck [15],

We can start from right in order to obtain

$$\begin{aligned} c_{\sigma_1\dots\sigma_L} &= \Psi_{(\sigma_1\dots\sigma_{L-1}),\sigma_L} = \sum_{a_{L-1}} U_{(\sigma_1\dots\sigma_{L-1}),a_{L-1}} S_{a_{L-1},a_{L-1}}(V^\dagger)_{a_{L-1},\sigma_L} = \sum_{a_{L-1}} \Psi_{(\sigma_1\dots\sigma_{L-2}),(\sigma_{L-1}a_{L-1})} B^{\sigma_L}_{a_{L-1}} = \\ &= \sum_{a_{L-1},a_{L-2}} U_{(\sigma_1\dots\sigma_{L-2}),a_{L-2}} S_{a_{L-2},a_{L-2}}(V^\dagger)_{a_{L-2},(\sigma_{L-1}a_{L-1})} B^{\sigma_L}_{a_{L-1}} = \sum_{a_{L-2},a_{L-1}} \Psi_{(\sigma_1\dots\sigma_{L-3}),(\sigma_{L-2}a_{L-2})} B^{\sigma_{L-1}}_{a_{L-2},a_{L-1}} B^{\sigma_L}_{a_{L-1}} = \dots \end{aligned}$$

or consider

$$(\mathbb{K}^d)^L \xrightarrow{\text{flatten}^{-1}} \text{Mat}_{\mathbb{K}}(d^{L-1},d) \xrightarrow{\text{SVD}} U_{\mathbb{K}}(d^{L-1},r_{L-1})\times\text{diag}_{\mathbb{K}}(r_{L-1})\times U_{\mathbb{K}}(r_{L-1},d) \xrightarrow{\cong} \text{Mat}_{\mathbb{K}}(d^{L-2},dr_{L-1})\times(\text{Mat}_{\mathbb{K}}(r_{L-1},1))^d \xrightarrow{\text{SVD}}$$

$$c_{\sigma_1\dots\sigma_L} \xmapsto{\text{flatten}^{-1}} c_{\sigma_1\dots\sigma_L} = \Psi_{(\sigma_1\dots\sigma_{L-1}),\sigma_L} \xmapsto{\text{SVD}} c_{\sigma_1\dots\sigma_L} = \sum_{a_{L-1}}^{r_{L-1}} U_{(\sigma_1\dots\sigma_{L-1}),a_{L-1}} S_{a_{L-1},a_{L-1}}(V^\dagger)_{a_{L-1},\sigma_L} \xmapsto{\cong} \begin{gathered} U_{(\sigma_1\dots\sigma_{L-1}),a_{L-1}} S_{a_{L-1},a_{L-1}} = \Psi_{(\sigma_1\dots\sigma_{L-2}),(\sigma_{L-1}a_{L-1})} \\ (V^\dagger)_{a_{L-1},\sigma_L} = B^{\sigma_L}_{a_{L-1}} \\ c_{\sigma_1\dots\sigma_L} = \sum_{a_{L-1}} \Psi_{(\sigma_1\dots\sigma_{L-2}),(\sigma_{L-1},a_{L-1})} B^{\sigma_L}_{a_{L-1}} \end{gathered} \xmapsto{\text{SVD}}$$

$$\xrightarrow{\text{SVD}} U_{\mathbb{K}}(d^{L-2},r_{L-2})\times\text{diag}_{\mathbb{K}}(r_{L-2})\times U_{\mathbb{K}}(r_{L-2},dr_{L-1})\times(\text{Mat}_{\mathbb{K}}(r_{L-1},1))^d \xrightarrow{\cong} \text{Mat}_{\mathbb{K}}(d^{L-3},dr_{L-2})\times(\text{Mat}_{\mathbb{K}}(r_{L-2},r_{L-1}))^d\times(\text{Mat}_{\mathbb{K}}(r_{L-1},1))^d$$

$$\xmapsto{\text{SVD}} c_{\sigma_1\dots\sigma_L} = \sum_{a_{L-1},a_{L-2}} U_{(\sigma_1\dots\sigma_{L-2}),a_{L-2}} S_{a_{L-2},a_{L-2}}(V^\dagger)_{a_{L-2},(\sigma_{L-1}a_{L-1})} B^{\sigma_L}_{a_{L-1}} \xmapsto{\cong} \begin{gathered} U_{(\sigma_1\dots\sigma_{L-2}),a_{L-2}} S_{a_{L-2},a_{L-2}} = \Psi_{(\sigma_1\dots\sigma_{L-3}),(\sigma_{L-2}a_{L-2})} \\ (V^\dagger)_{a_{L-2},(\sigma_{L-1}a_{L-1})} = B^{\sigma_{L-1}}_{a_{L-2}a_{L-1}} \\ c_{\sigma_1\dots\sigma_L} = \sum_{a_{L-1},a_{L-2}} \Psi_{(\sigma_1\dots\sigma_{L-3}),(\sigma_{L-2},a_{L-2})} B^{\sigma_{L-1}}_{a_{L-2},a_{L-1}} B^{\sigma_L}_{a_{L-1}} \end{gathered}$$

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

(63) $$V^\dagger V = 1$$

, then

(64) $$\delta_{a_l a_l'} = \sum_{\sigma_m a_m} (V^\dagger)_{a_l(\sigma_m a_m)} V_{(\sigma_m a_m) a_l'} = \sum_{\sigma_m a_m} B^{\sigma_m}_{a_l a_m} \overline{B}^{\sigma_m}_{a_l' a_m} \Longrightarrow \sum_{\sigma_m} \boxed{B^{\sigma_m}(B^{\sigma_m})^\dagger = 1}$$

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**.

28.2.1. *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.

$$\begin{aligned} \mathrm{Mat}_{\mathbb{K}}(d^{L-1}, d) \xrightarrow{\text{SVD}} U_{\mathbb{K}}(d^{L-1}, r_{L-1}) \times \mathrm{diag}_{\mathbb{K}}(r_{L-1}) \times U_{\mathbb{K}}(r_{L-1}, d) &\xrightarrow{\cong} \mathrm{Mat}_{\mathbb{K}}(d^{L-2}, dr_{L-1}) \times (\mathrm{Mat}_{\mathbb{K}}(r_{L-1}, 1))^d \\ \Psi_{(\sigma_1\dots\sigma_{L-1}),\sigma_L} \xmapsto{\text{SVD}} = \textstyle\sum_{a_{L-1}}^{r_{L-1}} U_{(\sigma_1\dots\sigma_{L-1}),a_{L-1}} S_{a_{L-1},a_{L-1}} (V^\dagger)_{a_{L-1},\sigma_L} &\xmapsto{\cong} \begin{matrix} U_{(\sigma_1\dots\sigma_{L-1}),a_{L-1}} S_{a_{L-1},a_{L-1}} = \Psi_{(\sigma_1\dots\sigma_{L-2}),(\sigma_{L-1}a_{L-1})} \\ (V^\dagger)_{a_{L-1},\sigma_L} = B^{\sigma_L}_{a_{L-1}} \end{matrix} \end{aligned}$$

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 $l = 1$:

$$\begin{aligned} \{0,1\}^{L-1} &\xrightarrow{(\text{flatten})^{-1}} \{0, 1, \dots 2^{L-1} - 1\} \\ (\sigma_0, \sigma_1, \dots \sigma_{L-2}) &\xmapsto{(\text{flatten})^{-1}} I_{L-1} := \sigma_0 + 2\sigma_1 + \dots + 2^i\sigma_i + \dots + 2^{L-2}\sigma_{L-2} = \textstyle\sum_{i=0}^{L-2} 2^i \sigma_i \end{aligned}$$

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:

$$\begin{aligned} \mathrm{Mat}_{\mathbb{K}}(d^{L-1}, r_{L-1}) &\xrightarrow{(\text{flatten})^{-1}} \mathrm{Mat}_{\mathbb{K}}(d^{L-2}, dr_{L-1}) \\ (US)_{(\sigma_0\dots\sigma_{L-2}),a_{L-1}} &\xmapsto{(\text{flatten})^{-1}} \Psi_{(\sigma_0,\sigma_1,\dots\sigma_{L-3}),(\sigma_{L-2}a_{L-1})} \\ \{0, 1, \dots 2^{L-1}-1\} \times \{0, 1, \dots r_{L-1} - 1\} &\xrightarrow{(\text{flatten})^{-1}} \{0, 1, \dots 2^{L-2} - 1\} \times \{0, 1, \dots dr_{L-1} - 1\} \\ I_{L-1}, a_{L-1} &\xmapsto{(\text{flatten})^{-1}} I_{L-1} \mod 2^{L-2}, \tfrac{I_{L-1}}{2^{L-2}} + da_{L-1} \end{aligned}$$

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.

$$\text{Mat}_{\mathbb{K}}(d^{L-l},r_{L-l}) \xrightarrow{(\text{flatten})^{-1}} \text{Mat}_{\mathbb{K}}(d^{L-(l+1)},dr_{L-l})$$

$$(US)_{(\sigma_0\dots\sigma_{L-(l+1)}),a_{L-l}} \xmapsto{(\text{flatten})^{-1}} \Psi_{(\sigma_0,\sigma_1,\dots\sigma_{L-(l+2)}),(\sigma_{L-(l+1)}a_{L-l})}$$

$$\{0,1,\dots d^{L-l}-1\}\times\{0,1,\dots r_{L-l}-1\} \xrightarrow{(\text{flatten})^{-1}} \{0,1,\dots d^{L-(l+1)}-1\}\times\{0,1,\dots dr_{L-l}-1\}$$

$$I_{L-l},a_{L-l} \xmapsto{(\text{flatten})^{-1}} I_{L-l} \mod d^{L-(l+1)}, \frac{I_{L-l}}{d^{L-(l+1)}}+da_{L-l}$$

$$U_{\mathbb{K}}(r_{L-l},dr_{L-(l-1)}) \xrightarrow{(\text{flatten})^{-1}} (\text{Mat}_{\mathbb{K}}(r_{L-l},r_{L-(l-1)}))^d$$

$$(V^\dagger)_{a_{L-l},(\sigma_{L-l}a_{L-(l-1)})} \xmapsto{(\text{flatten})^{-1}} (V^\dagger)_{a_{L-l},(\sigma_{L-l}a_{L-(l-1)})} = B^{\sigma_{L-l}}_{a_{L-l},a_{L-(l-1)}}$$

$$\{0,1,\dots r_{L-l}-1\}\times\{0,1,\dots dr_{L-(l-1)}-1\} \xrightarrow{(\text{flatten})^{-1}} (\{0,1,\dots r_L-1\}\times\{0,1,\dots r_{L-(l-1)}-1\})^d$$

$$a_{L-l},(\sigma_{L-l}a_{L-(l-1)}) := a_{L-l},\sigma_{L-1}+da_{L-(l-1)} \xmapsto{(\text{flatten})^{-1}} a_{L-l},\frac{(\sigma_{L-1}a_{L-(l-1)})}{d}\,;\,\sigma_{L-l}=(\sigma_{L-l}a_{L-(l-1)}) \mod d$$

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 A. Cox. John Little. Donal O'Shea. **Using Algebraic Geometry**. Second Edition. Springer. 2005. ISBN 0-387-20706-6 QA564.C6883 2004
[3] David Cox, John Little, Donal O'Shea. **Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra**, Fourth Edition, Springer
[4] Schottenloher, Martin. **A Mathematical Introduction to Conformal Field Theory**. Springer, 2008.
[5] 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
[6] M. Hjorth-Jensen, **Computational Physics**, University of Oslo (2015) http://www.mn.uio.no/fysikk/english/people/aca/mhjensen/
[7] M.E.J. Newman and G.T. Barkema. **Monte Carlo Methods in Statistical Physics**. Oxford University Press. 1999.
[8] Glen E. Bredon. **Topology and Geometry**. Graduate Texts in Mathematics (Book 139). Springer; Corrected edition (October 17, 1997). ISBN-13: 978-0387979267
[9] Jean-Pierre Serre (Author), J. Stilwell (Translator). **Trees** (Springer Monographs in Mathematics) 1st ed. 1980. Corr. 2nd printing 2002 Edition. ISBN-13: 978-3540442370
[10] Joseph J. Rotman, **Advanced Modern Algebra** (Graduate Studies in Mathematics) 2nd Edition, American Mathematical Society; 2 edition (August 10, 2010), ISBN-13: 978-0821847411
[11] Edward Scheinerman. **C++ for Mathematicians: An Introduction for Students and Professionals**. 1st Edition. CRC Press; 1 edition (June 8, 2006). ISBN-13: 978-1584885849
[12] Jeffrey M. Lee. **Manifolds and Differential Geometry**, *Graduate Studies in Mathematics* Volume: 107, American Mathematical Society, 2009. ISBN-13: 978-0-8218-4815-9
[13] 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]**
[14] Ulrich Schollwoeck. *The density-matrix renormalization group. Rev. Mod. Phys.* **77**, 259 (2005) arXiv:cond-mat/0409292 **[cond-mat.str-el]**
[15] 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]**
[16] José L.F. Barbón and Eliezer Rabinovici. "Holographic Complexity And Spacetime Singularities." arXiv:1509.09291 **[hep-th]**
[17] Juan Maldacena, Leonard Susskind. "Cool horizons for entangled black holes." arXiv:1306.0533 **[hep-th]**
[18] Slava Rychkov. "EPFL Lectures on Conformal Field Theory in $D \geq 3$ Dimensions." arXiv:1601.05000 **[hep-th]**
[19] G. Evenbly, G. Vidal. "Tensor network states and geometry." arXiv:1106.1082 **[quant-ph]**
[20] Mark Van Raamsdonk. "Lectures on Gravity and Entanglement." arXiv:1609.00026 **[hep-th]**