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

Part 1. Algebra; Groups, Rings, R-Modules, Categories 1
1. Prime numbers, GCD (greatest common denominator), integers, Euler's totient, Chinese Remainder Theorem, integer divison, modulus, remainders; Euclid's Lemma 1
2. Groups; normal subgroups 3
3. R-modules 4
4. Categories; Category Theory 5

Part 2. Reading notes on Cox, Little, O'Shea's *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra* 8
5. Geometry, Algebra, and Algorithms 8
6. Groebner Bases 9
7. Elimination Theory 9
8. The Algebra-Geometry Dictionary 9
9. Polynomial and Rational Functions on a Variety 9
10. Robotics and Automatic Geometric Theorem Proving 9

Part 3. Reading notes on Cox, Little, O'Shea's *Using Algebraic Geometry* 9
11. Introduction 9
12. Solving Polynomial Equations 11
13. Resultants 11
14. Computation in Local Rings 11
15. 12
16. 12
17. Polytopes, Resultants, and Equations 12
18. Polyhedral Regions and Polynomials 12
19. Algebraic Coding Theory 13
20. The Berlekamp-Massey-Sakata Decoding Algorithm 13

Part 4. Conformal Field Theory : Virasoro Algebra 13

Part 5. Algebraic Topology 14
21. Simplicial Complexes 14

Part 6. Graphs, Finite Graphs 14
22. Graphs, Finite Graphs, Trees 14
References 17

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) [1].

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

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

Theorem 1 (1.7 of Rotman (2010) [1]). *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.*

$$d = sa + tb$$

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

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 $c \in I$.

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

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 2 (**Euclid's Lemma**; 1.10 of Rotman (2010) [1]). *If p prime and $p|ab$, then $p|a$ or $p|b$.*

More generally,
if prime p divides product $a_1 a_2 \dots a_n$,
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. $a_1 a_2 \dots a_n / p \in \mathbb{Z}$,
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. 1,

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

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) [1]). *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 3 (1.26 of Rotman (2010) [1]). *If $\gcd(a, m) \equiv (a, m) = 1$, then $\forall\, b \in \mathbb{Z}$, $\exists\, x$ s.t.*

$$ax = b \mod m$$

In fact, $x = sb$, where $sa \equiv 1 \mod m$

Proof. $\gcd(a, m) = 1 = sa + tm$.

Then $b = b \cdot 1 = b(sa + tm) = sab + tmb$ or $b = tbm + sab$ or $a(sb) = -tbm + b$.

So $a(sb) \mod m = b$.

Let $x := sb$ and so $ax \mod m = b$.

Now suppose $x \neq sb$ s.t. $ax \mod m = b$. Then $ax = qm + b$. From $a(sb) \mod m = b$, we also get $a(sb) = q'm + b$. Then $a(x - sb) \mod m = 0$, 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 $(sb) \mod m = x$. □

Proposition 1 (3.1 of Scheinerman (2006) [?]). *Let $a, b \in \mathbb{Z}$, let $c = a \mod b$, i.e. $a = qb + c$ s.t. $0 \leq c < b$.*

Then

$$gcd(a, b) = gcd(b, c) \tag{1}$$

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

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.

Definition 1. *if $a, b \in \mathbb{Z}$,*
*a **divisor** of b, if $\exists\, d \in \mathbb{Z}$ s.t. $b = ad$.*
*Also, a **divides** b or b multiple of $a \equiv a|b$.*
$a|b \equiv b/a \in \mathbb{Z}$

cf. pp. 3 of Ch. 1 Things Past, Sec. 1.1 Some Number Theory of Rotman (2010) [1].
cf. Ch. 5 Arrays, Sec. 5.1 Euler's totient of Scheinerman (2006) [?]
For

$\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$

$\varphi : n \mapsto \varphi(n) :=$ number of elements of $\{1, 2, \dots n\}$ that are relative prime to n $= |\{i | i \in \{1, 2, \dots n\}, (n, i) = 1$ 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 2 (5.1). *Let p prime, $n \in \mathbb{Z}^+$*

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

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

By Prop. 1,

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

Scheinerman (2006) [?]

1.2.1. *Chinese Remainder Theorem.*

Theorem 4. *If m, m' relatively prime (i.e. $\gcd(m,m')=1$), then for*
$$x \equiv b \mod m$$
$$x \equiv b' \mod m'$$
i.e. given $b, b'm, m'$, and wanting to find x, $\exists x$ and $\forall 2x$'s, $x = x' \mod mm'$.

Proof. $x = b'ms + bm's'$ □

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

2. Groups; normal subgroups

Definition 2 (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 3 (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 4 (exact sequence of groups)**.** ***exact sequence*** *if $imf_{n+1} = kerf_n \qquad \forall n$ for sequence of group homomorphisms and groups*

$$G_{n+1} \xrightarrow{f_{n+1}} G_n \xrightarrow{f_n} G_{n-1} \tag{2}$$

Theorem 5. (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) $\mathrm{im}(1 \to A) = 1$, since $1 \to A$ is a group homomorphism ($(1 \to A)(1) = 1_A$).
if $1 \to A \xmapsto{f} B$ exact, $\ker f = \mathrm{im}(1 \to A) = 1$, so if $f(x) = 1$, $x = 1$, f injective.
If f injective, $\ker f = 1$. $1 = \mathrm{im}(1 \to A)$. $1 \to A \xmapsto{f} B$, exact.
(2) $\ker(C \to 1) = C$, by def. of $C \to 1$
if $B \xmapsto{g} C \to 1$ exact, $\mathrm{im} g = g(B) = \ker(C \to 1) = C$. $g(B) = C$ implies g surjective.
If g surjective, $g(B) = C = \ker(C \to 1)$. $B \xmapsto{g} C \to 1$ exact.
(3) From (i), $1 \to A \xmapsto{h} B$ exact iff h injective. From (ii), $A \xmapsto{h} B \to 1$, exact iff h surjective.
h isomorphism.

□

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

Theorem 6 (1st Isomorphism Theorem (Modules) Thm. 7.8 of Rotman (2010) [1])**.** *If $f : M \to N$ is R-map of modules, then $\exists$ R-isomorphism s.t.*

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

$$\begin{aligned} \varphi &: M/kerf \to imf \\ \varphi &: m + kerf \mapsto f(m) \end{aligned} \tag{3}$$

Proof. View M, N as abelian groups.

Recall natural map $\begin{aligned} \pi &: M \to M/N \\ m &\mapsto m + N \end{aligned}$
Define φ s.t. $\varphi\pi = f$.
(φ well-defined). Let $m + \ker f = m' + \ker f$, $m, m' \in M$, then $\exists n \in \ker f$ s.t. $m = m' + n$.
$$\varphi(m + \ker f) = \varphi\pi(m) = f(m) = f(m' + n) = f(m') + f(n) = \varphi\pi(m') + 0 = \varphi(m' + \ker f)$$
$\implies \varphi$ well-defined.
(φ surjective). Clearly, $\mathrm{im}\varphi \subseteq \mathrm{im} f$.
Let $y \in \mathrm{im} f$. So $\exists m \in M$ s.t. $y = f(m)$. $f(m) = \varphi\pi(m) = \varphi(m + \ker f) = y$. So $y \in \mathrm{im}\varphi$. $\mathrm{im} f \subseteq \mathrm{im}\varphi$.
$\implies \varphi$ surjective.
(φ injective) If $\varphi(a + \ker f) = \varphi(b + \ker f)$, then
$$\varphi\pi(a) = \varphi\pi(b) \text{ or } f(a) = f(b) \text{ or } 0 = f(a) - f(b) = f(a-b) \text{ so } a - b \in \ker f(a-b) + \ker f = \ker f \text{ so } a + \ker f = b + \ker f$$
φ isomorphism.
φ R-map. $\varphi(r(m + N)) = \varphi(rm + N) = f(rm)$.
Since f R-map, $f(rm) = rf(m) = r\varphi(m + N)$. φ is R-map indeed.

□

Theorem 7 (2nd Isomorphism Theorem (Modules) Thm. 7.9 of Rotman (2011) [1])**.** *If S, T are submodules of module M, i.e. $S, T \in M$, then $\exists$ $R-$isomorphism*

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

$$S/(S \cap T) \to (S+T)/T \tag{4}$$

Proof. Let natural map $\pi : M \to M/T$.

So $\ker\pi = T$.

Define $h := \pi|_S$, so $h : S \to M/T$, so $\ker h = S \cap T$,

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

i.e. $(S+T)/T$ consists of all those cosets in M/T having a representation in S.

By 1st. isomorphism theorem,

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

□

Theorem 8 (3rd Isomorphism Theorem (Modules) Thm. 7.10 of Rotman (2011) [1])**.** *If $T \subseteq S \subseteq M$ is a tower of submodules, then $\exists$ R-isomorphism*

$$\begin{tikzcd} M/T \arrow[r, "g"] \arrow[d, "\pi"] & M/S \\ (M/T)/(S/T) = (M/T)/\ker g \arrow[ur, "\cong"] & \end{tikzcd}$$

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

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

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

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

$\ker g = S/T$ since

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

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

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

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

3. R-modules

Definition 5 (R-homomorphism (or R-map))**.** *If ring R, R-modules M, N, then function $f : M \to N$, if $\forall m, m' \in M$, $\forall r \in R$,*

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

Definition 6 (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

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

natural map

(7) $$\begin{aligned} & \pi : M \to M/N \\ & m \mapsto m + N \end{aligned}$$

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 3 (7.15 of Rotman (2010) [1])**.** (i) $S \coprod T \simeq M$

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

(8) $$\begin{aligned} & M = im(i) + im(j) \text{ and} \\ & im(i) \bigcap im(j) = \{0\} \end{aligned}$$

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

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

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

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

with $m = is + jt$.

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

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

s.t.

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

Proof.
- (i)$\to$ (ii) Given $S \coprod T \simeq M$,

let $\varphi : S \coprod T \to M$ be this isomorphism.

Define

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

i, j are injections, being composites of injections.

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

Then

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

Let $c \in \text{im}(i) + \text{im}(j)$. Since $\begin{matrix} i : S \to M \\ j : T \to M \end{matrix}$, $c \in M$.

$\Longrightarrow M = \text{im}(i) + \text{im}(j)$.

If $x \in \text{im}(i) \bigcap \text{im}(j)$,

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

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

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

- (ii)→ (iii) Given $\begin{matrix} i : S \to M \\ j : T \to M \end{matrix}$, s.t. $M = \text{im}(i) + \text{im}(j)$, so

  $\forall m \in M$, $m = i(s) + j(t)$ for some $s \in S, t \in T$.

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

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

So $s = s', t = t'$, since i, j injective.

- (iii)→ (iv)
  Given $\forall m \in M$, $\exists ! s \in S, t \in T$ s.t.

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

Define

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

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

4. Categories; Category Theory

4.1. **Categories.** cf. 7.2 Categories of Rotman (2010) [1]

4.1.1. *Russell paradox, Russell set.*

Definition 7 (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 8 (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*

$$Hom(A,B) \times Hom(B,C) \to Hom(A,C)$$
$$(f,g) \mapsto gf$$

, s.t.

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

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

In summary,

$$\mathbf{C} := (Obj(\mathbf{C}), Mor\mathbf{C}, \circ, \mathbf{1}) \equiv (Obj\mathbf{C}, Mor\mathbf{C}, \circ_{\mathbf{C}}, \mathbf{1}_{\mathbf{C}}) \quad (9)$$

s.t.

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

Examples (7.25 of Rotman (2010)[1]):

(i) $\mathbf{C} = \text{Sets}$
(ii) $\mathbf{C} = \text{Groups} = \text{Grps}$
(iii) $\mathbf{C} = \text{CommRings}$
(iv) $\mathbf{C} = {}_R\mathbf{Mod}$, if $R = \mathbb{Z}$, ${}_\mathbb{Z}\mathbf{Mod} = \mathbf{Ab}$, i.e. $\mathbb{Z}-$modules are just abelian groups.
(v) $\mathbf{C} = \mathbf{PO}(X)$, If partially ordered set X, regard X as category, s.t. $\mathbf{Obj}, \mathbf{PO}(X) = \{x | x \in X\}$, $\forall \text{Hom}(x,y) \in \mathbf{Mor_{PO}}(X)$, $\text{Hom}(x,y) = \begin{cases} \emptyset & \text{if } x \not\preceq y \\ \kappa^x_y & \text{if } x \preceq y \end{cases}$ 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 9 (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.*

$$gf = 1_A$$
$$fg = 1_B$$

*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 10 (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

$A' = A \times \{1\}$.
$B' = B \times \{2\}$

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

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

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

From Rotman (2010) [1], pp. 447,

Definition 11. ***coproduct*** *$A \coprod B \equiv C \in Obj(\mathcal{C})$*

In my notation,
coproduct

$$\begin{matrix} (\mu_1, A_1 \coprod A_2) \\ (\mu_2, A_1 \coprod A_2) \end{matrix} \quad (10)$$

where injection (morphisms)

$$\begin{matrix} \mu_1 : A_1 \to A_1 \coprod A_2 \\ \mu_2 : A_1 \to A_1 \coprod A_2 \end{matrix} \quad (11)$$

s.t.

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

then

$$\begin{gathered} \exists ! [f_i] \equiv [f_1, f_2] \in \text{Mor}\mathbf{A},\, [f_1, f_2] : A_1 \coprod A_2 \to A \text{ s.t.} \\ [f_1, f_2]\mu_1 = f_1 \\ [f_1, f_2]\mu_2 = f_2 \end{gathered} \tag{12}$$

i.e.

$$\begin{tikzcd} & & A \\ A_1 \arrow[urr, "f_1"] \arrow[rr, "\mu_1"] & & A_1 \coprod A_2 \arrow[u, dashed, "{[f_1,f_2]}"'] \\ A_2 \arrow[uurr, "f_2"] \arrow[urr, "\mu_2"'] & & \end{tikzcd} \tag{13}$$

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

$$\begin{gathered} \exists ! \, [f_i] \equiv [f_i]_{i\in I} \in \text{Mor}\mathbf{A},\, [f_i] : \coprod_{i\in I} A_i \to A \text{ s.t.} \\ [f_i]\mu_j = f_j \qquad \forall\, j \in I \end{gathered} \tag{14}$$

i.e.

$$\begin{tikzcd} & A \\ A_j \arrow[ur, "f_j"] \arrow[r, "\mu_j"'] & \coprod_{i\in I} A_i \arrow[u, dashed, "{[f_i]}"'] \end{tikzcd} \tag{15}$$

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 12 (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

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

4.1.2. *Examples of extra assumptions on sets,* ${}_R$***Mod*** *we take for granted.* In Prop. 7.15(iii) Rotman (2010) [1],

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

$$ip + jq = 1_M$$

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

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

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 13 (free products). ***free products*** *are coproducts in groups*

Prop. 7.26, Rotman (2010) [1]

Proposition 4 (7.26, Rotman). *If* A, B *are* R*-modules,*
then their coproducts in ${}_R$***Mod*** *exists, and it's the direct sum* $C = A \coprod B$*.*

Proof. Define

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

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

Define

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

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

so diagram commutes, i.e.

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

If $\psi : C \to X$ makes diagram commute,

$$\psi((a,0)) = f(a) \qquad \forall\, a \in A$$
$$\psi((0,b)) = g(b) \qquad \forall\, b \in B$$

and since ψ is a homomorphism, $\psi((a,b)) = \psi((a,0)) + \psi((0,b)) = f(a) + g(b) = \theta((a,b))$. $\psi = \theta$.

Prop. 7.27, Rotman (2010) [1]

Proposition 5 (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 $\mu_A : A \to C,\ \mu_B : B \to C$, $\nu_A : A \to D,\ \nu_B : B \to D$

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

Just substitute $X = D$ in diagram above.

Then substitute again:

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

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

Then C, D are equivalent. □

Exer. 7.29 on pp. 459 of Rotman (2010) [1]

Definition 14. *If $A, B \in Obj\mathbf{C}$, then their **product**; $A \prod B = P \in Obj\mathbf{C}$, and morphisms $p : P \to A$, $q : P \to B$ s.t. $\forall\, X \in Obj\mathbf{C}$,*

$\forall\ f : X \to A \in Mor\mathbf{C}$,
$g : X \to B \in Mor\mathbf{C}$
$\exists!\, \theta : X \to P$, 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) [2],

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

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

$$\prod_i X_i := \varprojlim \alpha \tag{16}$$

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

$$p : A \times B \to A \qquad q : A \times B \to B$$
$$p(a,b) \mapsto a \qquad q(a,b) \mapsto b$$

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 6 (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 $\begin{aligned} p_A &: C \to A, \quad & q_A &: D \to A \\ p_B &: C \to B, & q_B &: D \to B \end{aligned}$

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

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. □

4.1.3. *Products of Modules and Sets.*

Proposition 7 (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*

$$A \sqcap B \cong A \sqcup B \tag{17}$$

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

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

If module X, since $\begin{aligned} f &: X \to A \\ g &: X \to B \end{aligned}$ 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 15. *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:*

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

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

cf. Thm. 7.32 of Rotman (2010) [1]

Theorem 9 (7.32, Rotman)**.** *Let commutative ring R.
$\forall$ R-module A, $\forall$ family $\{B_i | i \in I\}$ of R-modules,*

$$Hom_R(A, \coprod_{i \in I} B_i) \simeq \coprod_{i \in I} Hom_R(A, B_i) \tag{18}$$

via R-isomorphism

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

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

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

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

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

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

So φ is R-map.
If $(f_i) \in \coprod_i \text{Hom}_R(A, B_i)$, then $f_i : A \to B_i$ $\forall i$
By Rotman's Prop. 7.31 (If family of R-modules $\{A_i | i \in I\}$, then direct product $C = \coprod_{i \in I} A_i$ is their product in ${}_R\mathbf{Mod}$),
By def. or product, $\exists!$ R-map , $\theta : A \to \coprod_{i \in I} B_i$ s.t. $p_i\theta = f_i$ $\forall i$

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

Then

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

, and so φ *surjective.*

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

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

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*

5. Geometry, Algebra, and Algorithms

5.1. Polynomials and Affine Space.

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

Definition 16 (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)

5.2. Affine Varieties.

5.3. Parametrizations of Affine Varieties.

5.4. Ideals.

5.5. Polynomials of One Variable.

6. Groebner Bases

6.1. Introduction.

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

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

6.4. Monomial Ideals and Dickson's Lemma.

6.5. The Hilbert Basis Theorem and Groebner Bases.

6.6. Properties of Groebner Bases.

6.7. Buchberger's Algorithm.

7. Elimination Theory

7.1. The Elimination and Extension Theorems.

7.2. The Geometry of Elimination.

8. The Algebra-Geometry Dictionary

8.1. Hilbert's Nullstellensatz.

8.2. Radical Ideals and the Ideal-Variety Correspondence.

9. Polynomial and Rational Functions on a Variety

9.1. Polynomial Mappings.

10. Robotics and Automatic Geometric Theorem Proving

10.1. 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

11. Introduction

11.1. Polynomials and Ideals. *monomial*

$$x_1^{\alpha_1} \dots x_n^{\alpha_n} \quad (1.1) \quad (19)$$

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 17 (1.3). *Let $f_1 \dots f_s \in k[x_1 \dots x_n]$*
Let $\langle f_1 \dots f_s \rangle = \{ p_1 f_1 + \dots + p_s f_s | p_i \in k[x_1 \dots x_n]$ for $i = 1 \dots s\}$

Exercise 1.

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

(b)

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

and for $pxy = (py)x$

(c)

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

Exercise 2.

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

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

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

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

Done.

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

Definition 18 (1.5). *Let $I \subset k[x_1 \dots x_n], \quad I \neq \emptyset$*
I ideal if

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

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

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

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

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

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

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

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

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

Definition 19 (1.6).

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

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

11.2.

11.3. Gröbner Bases.

Definition 20 (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 LT(I)

11.4. **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 21 (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 $f + g \in I \quad \forall f, g \in I$

$$pf \in I, \quad \forall f \in I \text{ arbitrary } p \in k[x_1 \dots x_n]$$

Let $f, g \in I(V)$

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

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

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

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

Exercise 4. $\quad I \subset \sqrt{I}$
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 $f \in \sqrt{I}$, $\quad I \subset \sqrt{I}$
Hilbert basis thm., $\forall$ ideal $I \subset k[x_1 \dots x_n]$ s.t. $I = \langle f_1 \dots f_s \rangle$
$\{ {}^{V(I) = \{(a_1 \dots a_n) | (a_1 \dots a_n) \in k^n, f_1(a_1 \dots a_n) = \dots = f_s(a_1 \dots a_n) = 0} \}$
$\mathbf{I}(\mathbf{V}(I)) = \{f \in k[x_1 \dots x_n] | f(a_1 \dots a_n) = 0 \quad \forall (a_1 \dots a_n) \in V(I)\}$
Let $g \in \sqrt{I}$, $\quad g^m \in I$, $\quad g^m = g^{m-1} g$
$g^m(a_1 \dots a_n) = 0 = g^{m-1}(a_1 \dots a_n) g(a_1 \dots a_n) = 0$. Then $g(a_1 \dots a_n) = 0$ or $g^{m-1}(a_1 \dots a_m) = 0$
as $g^m \in I$, and $V(I)$ is s.t. $f_1(a_1 \dots a_n) = \dots = f_s(a_1 \dots a_n) = 0$ for $I = \langle f_1 \dots f_s \rangle$

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

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

- (Ideal-variety correspondence) Let k arbitrary field

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

Additional Exercises for Sec.4. Exercise 6.

12. Solving Polynomial Equations

12.1.

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

$$f = h_1 g_1 + \dots + h_t g_t + \overline{f}^G \qquad (2.1) \qquad (20)$$

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

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

algebraic

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

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

12.3.

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

13. Resultants

14. Computation in Local Rings

14.1. Local Rings.

Definition 22 (1.1).

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

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

Proposition 8 (1.2). *Let $R = k[x_1 \dots x_n]_{\langle x_1 \dots x_n \rangle}$. Then*

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

Exercise 1. if $p = (a_1 \dots a_n) \in k^n$, $R = \{ \frac{f}{g} | f, g \in k[x_1 \dots x_n], \, g(p) \neq 0 \}$

(a) R subring of field of rational functions $k(x_1 \dots x_n)$
(b) Let M ideal generated by $x_1 - a_1 \dots x_n - a_n$ in R
Then $\forall \frac{f}{g} \in R \backslash M$, $\frac{f}{g}$ unit in R (i.e. multiplicative inverse in R)
(c) M maximal ideal in R

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

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

$f = \frac{f}{1} \in R, \quad \forall f \in k[x_1 \dots x_n]$, so $k[x_1 \dots x_n] \subset R$

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

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

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

Prop. 1.2. properties

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

Definition 23 (1.3). *local ring is a ring that has exactly 1 maximal ideal*

Proposition 9 (1.4). *ring R with proper ideal $M \subset R$ is local ring if $\forall \frac{f}{g} \in R \backslash M$ is unit in R*

localization Ex. 8, Ex. 9
parametrization
Exercise 2.

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

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

$$k\{x_1 \dots x_n\} = \{ \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha | c_\alpha \in k, \text{ series converges in some open } U \ni 0 \in k^n \} \quad (1.5) \tag{21}$$

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

$$k[[x_1 \dots x_n]] = \{ \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha | c_\alpha \in k \} \text{ series need not converge} \quad (1.6) \tag{22}$$

variety V

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

14.2. 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 24 (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, $m(p) = \dim k[x_1 \dots x_n]_M / Ik[x_1 \dots x_n]_M$

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

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

15.

16.

17. Polytopes, Resultants, and Equations

18. Polyhedral Regions and Polynomials

18.1. 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?

(23)
$$\begin{aligned} 4A+5B &\leq 37 \\ 2A+3B &\leq 20 \\ A, B &\in \mathbb{Z}^*_{\geq 0} \end{aligned} \tag{1.1}$$

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"

(24)
$$a_{ij}A_j = b_i, \quad A_j \in \mathbb{Z}_{\geq 0} \tag{1.4}$$

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 10 (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 11 (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.

18.2. Integer Programming and Combinatorics.

19. Algebraic Coding Theory

20. The Berlekamp-Massey-Sakata Decoding Algorithm

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

Part 4. Conformal Field Theory : Virasoro Algebra

cf. Schottenloher (2008) [?]

Definition 25. ***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) [?].

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 im$i$ is in center of E, i.e. $a \in A, b \in E \Longrightarrow i(a)b = bi(a)$.

20.0.1. *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

$$1 \longrightarrow \mathbb{Z}/k\mathbb{Z} \longrightarrow E \times U(1) \xrightarrow{\pi} U(1) \longrightarrow 1 \tag{25}$$

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

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

Part 5. Algebraic Topology

cf. Bredon (1997) [5]

21. Simplicial Complexes

cf. pp. 245, from Sec. 21 Simplicial Complexes of Ch. 4 Homology Theory in Bredon (1997) [5]
$\mathbf{v}_0, \dots \mathbf{v}_n \in \mathbb{R}^\infty$, "affinely independent" if they span an affine n-plane, i.e.

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

If not, then, e.g. $\lambda_0 \neq 0$, assume $\lambda_0 = -1$, and solve the equations to get

$$\begin{gathered} \mathbf{v}_0 = \sum_{i=1}^n \lambda_i \mathbf{v}_i \\ \sum_{i=1}^n \lambda_i = 1 \end{gathered}$$

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

$$\sigma = (\mathbf{v}_0, \dots \mathbf{v}_n) = \{ \sum_{i=0}^n \lambda_i \mathbf{v}_i | \sum_{i=0}^n \lambda_i = 1, \lambda_i \geq 0 \} \tag{26}$$

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 26. *(geometric) simplicial complex $K :=$ collection of affine simplices s.t.*

1. *$\sigma \in K \Longrightarrow$ any face of $\sigma \in K$; and*
2. *$\sigma, \tau \in K \Longrightarrow \sigma \bigcap \tau$ is a face of both σ and τ, or $\sigma \bigcap \tau = \emptyset$*

If K simplicial complex, $|K| = \bigcup \{\sigma | \sigma \in K\} \equiv$ "polyhedron" of K

Definition 27 (Def. 21.2 of Bredon (1997) [5])**.** *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) [5].
Then this gives CW-complex structure on $|K|$ with f_σ as characteristic maps.

Part 6. Graphs, Finite Graphs

22. Graphs, Finite Graphs, Trees

Serre (1980) [6]
cf. Chapter I. Trees and Amalgams, Section 1 Amalgams, Subsection 1.1 Direct limits of Serre (1980) [6]
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 $\{h_i | h_i : G_i \to H; h_j \circ f = h_i \quad \forall f \in F_{ij}\}$,
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}.

Proposition 12. $\exists !$ *pair* G, *family* $(f_i)_{i\in I}$, *i.e. (pair consisting of* $G, (f_i)_{i\in I}$, *unique up to unique isomorphism.*

Proof. Define G by generators and relations.
Take generating family to be disjoint union of those for G_i.
relations - xyz^{-1} where $x,y,z\in G_i$, $z = xy \in G_i$
xy^{-1} where $x \in G_i$, $y \in G_j$, $y = f(x)$ for at least $f \in F_{ij}$.
Thus, existence of $G, \{f_i\}$.
G represents functor $H \mapsto \varprojlim \mathrm{Hom}(G_i, H)$.
Thus, uniqueness (also from universal property). □

e.g. groups A, G_1, G_2, homomorphisms $f_1 : A \to G_1$.
$f_2 : A \to G_2$
G obtained by amalgamating A in G_1, G_2 by $f_1, f_2 \equiv G_1 *_A G_2$.
1 can have $G = \{1\}$, even though f_1, f_2 non-trivial.
Application: (Van Kampen Thm.)
Let topological space X be covered by open U_1, U_2.
Suppose $U_1, U_2, U_{12} = U_1 \bigcap U_2$ arcwise connected.
Let basept. $x \in U_{12}$.
Then $\pi_1(X;x)$ obtained by taking 3 groups

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

and amalagamating them according to homomorphism

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

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

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

$$A^n = \text{subgroup of } A \text{ generated by } f_1^{-1}(G_1^{n-1}) \text{ and } f_2^{-1}(G_2^{n-1})$$
$$G_1^n = \text{subgroup of } G_i \text{ generated by } f_i(A^n)$$

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) [6]
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.

22.0.1. *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.

$$i_m \neq i_{m+1} \text{ for } 1 \leq m \leq n-1 \tag{27}$$

cf. (T) of Serre (1980) [6].
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 28 (reduced word)**.** ***reduced word*** *of type* $\mathbf{i}$, m,

$$m = (a; s_1 \dots s_n) \tag{28}$$

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 10 (1 of Serre (1980) [6])**.** $\forall g \in G$, $\exists$ *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 $g \in G$

$$g = a s_1 \dots s_n, \quad a \in A, \; s_1 \in S_{i_1} - \{1\} \dots s_n \in S_{i_n} - \{1\}$$

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) [6]

Definition 29 (1. of Serre (1980) [6])**.** ***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_+

22.0.2. *Realization of a Graph.* cf. Realization of a Graph in Serre (1980) [6].
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

$$\begin{aligned} & (y,t) \equiv (\overline{y}, 1-t) \\ & (y,0) \equiv o(y) \qquad \forall y \in Y, \forall t \in [0,1] \\ & (y,1) \equiv t(y) \end{aligned} \tag{29}$$

quotient space real$(\Gamma) = T/R$ is *realization* of graph Γ. (realization is a functor which commutes with direct limits).
Let $n \in \mathbb{Z}^+$. Consider oriented graph of $n+1$ vertices $0, 1, \dots n$,

Definition 30. *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 31 (connected graph; Def. 3 of Serre (1980) [6]). *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.*

22.0.3. *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 32 (circuit; Def. 4 of Serre (1980) [6]). *circuit (length n) in graph is subgraph isormorphic to $Circ_n$.*

i.e. subgraph = path $(y_1 \dots y_n)$, without backtracking, s.t. $P_i = t(y_i)$, $(1 \leq i \leq n)$ distinct, s.t. $P_n = o(y_1)$

$n = 1$ case: Circ_1, $\mathbb{Z}/\mathbb{Z} = \{0\}$, 1 edge, $[0,1]$, $0 \in \mathbb{Z}/1\mathbb{Z}$, $\begin{aligned} & o([0,1]) = 0 \\ & t([0,1]) = 1 \end{aligned}$

Note Circ_1 has automorphism of order 2, which changes its orientation, i.e.
$\exists$ automorphism $\sigma \in \text{Aut}(\text{Circ}_1)$ s.t. $|\sigma| = 2$, i.e. $\sigma^2 = 1$.
loop := circuit of length 1; so loop $\in \overline{\text{Circ}_1}$.

path (y_1), $P_1 = t(y_1) = o(y_1)$.

$n = 2$ case: Circ_2, $\mathbb{Z}/2\mathbb{Z} = \{0,1\}$, 2 edges $[0,1], [1,2]$,

path (y_1, y_2), $(1 \leq i \leq 2)$, $\begin{aligned} & P_1 = t(y_1) \\ & P_2 = t(y_2) = o(y_1) \end{aligned}$

22.1. **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 $\begin{aligned} & \overline{(P,Q)} = (Q,P) \\ & o(P,Q) = P \\ & t(P,Q) = Q \end{aligned}$

In this graph, 2 edges with same origin and same terminus are equal. This is equivalent to (see following Def.)

Definition 33 (combinatorial; Def. 5 of Serre (1980) [6]). *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.

References

[1] Joseph J. Rotman, **Advanced Modern Algebra** (Graduate Studies in Mathematics) 2nd Edition, American Mathematical Society; 2 edition (August 10, 2010), ISBN-13: 978-0821847411
[2] 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
[3] David A. Cox. John Little. Donal O'Shea. **Using Algebraic Geometry**. Second Edition. Springer. 2005. ISBN 0-387-20706-6 QA564.C6883 2004
[4] David Cox, John Little, Donal O'Shea. **Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra**, Fourth Edition, Springer
[5] Glen E. Bredon. **Topology and Geometry**. Graduate Texts in Mathematics (Book 139). Springer; Corrected edition (October 17, 1997). ISBN-13: 978-0387979267
[6] Jean-Pierre Serre (Author), J. Stilwell (Translator). **Trees** (Springer Monographs in Mathematics) 1st ed. 1980. Corr. 2nd printing 2002 Edition. ISBN-13: 978-3540442370