SEOUL NATIONAL UNIVERSITY, DEPARTMENT OF MATHEMATICS

Graduate Algebra 2 Lecture Note by Insuk Lee

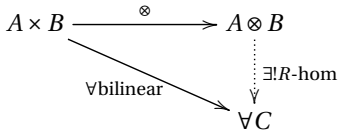
Hanbaek Lyu

December 6, 2012

1 MULTILINEAR ALGEBRA

Notation. R : commutative ring with 1. A, B, C, M, V : (unitary) R-module

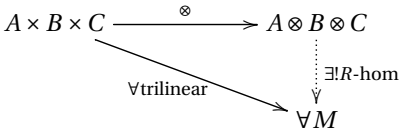
Definition 1. The tensor product $A \otimes_R B$ is defined by the universal property



Existence? Consider it as the quotient of the free group : $A \otimes B = \mathscr{F}(A \times B)/(\text{bilinearity})$.

Exercise 1. Show that $(A \otimes B) \otimes C \approx A \otimes (B \otimes C)$.

Definition 2. Tensor product $A \otimes B \otimes C$ is defined by the following universal property



HW 1. Show that the exsistence of the tensor product $A \otimes B \otimes C$ follows from Exercise 1.

Definition 3. One can define similarly the tensor product of n R-moduels: $A_1 \otimes A_2 \otimes \cdots \otimes A_n$.

Associativity "$a(bc) = (ab)c$" implies the general associativity : order of parenthesis doesn't matter. For instance, $(ab)(cd(ef)) = a((bc)d)ef$

Definition 4. Let V be an R-module. Define the tensor algebra $T(V)$ by

$$\begin{aligned} T(V) &= \bigoplus_{i\in\mathbb{Z}^+} T^i(V) \\ &= R \oplus V \oplus (V\otimes V) \oplus (V\otimes V\otimes V) \oplus \cdots \end{aligned}$$

where $T^0(V) = R$, $T^i(V) = T^{i-1}(V)\otimes V$.

$\mathbb{Z}^+$ denotes the set of nonnegative integers. Note that $T(V)$ is a graded algebra.

Example 1. $(A\otimes B)\otimes C$

We need to define multiplication in order to make $T(V)$ into an algebra. We simply make the tensor product into the multiplication. For example, for $u, v, w \in V$, define $u\cdot v = u\otimes v$, and $u\cdot(v\otimes v) = u\otimes v\otimes w$.
A multiplication is a R-bilinear map $T(V)\times T(V)\to T(V)$ which is associative. Does this map exists? Not so sure. But consider instead each direct summand. On can define following bilinear map

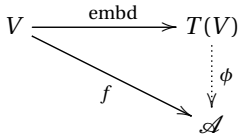
$$T^i(V)\times T^j(V) \longrightarrow T^{i+j}(V)$$

by $(u, v)\mapsto u\otimes v$, that is, the tensor map $\otimes$.
Associativity is clear:

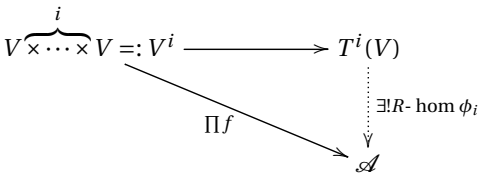
$$T^i(V)\times T^j(V)\times T^k(V) \longrightarrow T^{i+j+k}(V)$$

Now we have multiplication on each direct summands. Linearly extend this to the multiplication of the whole.

Universal property of tensor algebra. Tensor algebra can be defined by the following universal property: for any R-algebra $\mathscr{A}$ and R-linear map $f : V\to\mathscr{A}$, there exists a unique R-algebra homomorphism $\phi : T(V)\to\mathscr{A}$ such that following diagram commutes;



where the horizontal map is the embedding onto the first summand $V\to T^1(V) = V$. To show this, note that for each direct summand $T^i(V)$, there is a unique R-algebra homomorphism $\phi_i : T^i(V)\to\mathscr{A}$ for which the following diagram commutes, by the universal property of tensor product:



That is, for each $(u_1, \cdots, u_i) \in V^i$,

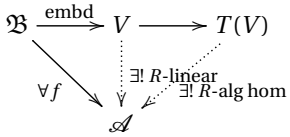
$$f(u_1)f(u_2)\cdots f(u_i) = \phi_i(u_1 \otimes u_2 \otimes \cdots \otimes u_i).$$

Then $\phi := \bigoplus_{i\in\mathbb{Z}^+} \phi_i : T(V) \to \mathscr{A}$ is an R-homomorphism for which the first diagram commutes. Is ϕ also an R-algebra homomorphism? It suffices to check for each direct summands since we have defined the multiplication on the tensor algebra by linearly extending the one on each summands. That is, we need to show that $\phi_i(a_i)\phi_j(b_j) = \phi_{i+j}(a_i b_j)$. Indeed, if we write $a_i = u_1 \otimes \cdots \otimes u_i \in T^i(V)$ and $b_j = v_1 \otimes \cdots \otimes v_j \in T^j(V)$, then

$$\begin{aligned} \phi_i(a_i)\phi_j(b_j) &= f(u_1)\cdots f(u_i)f(v_1)\cdots f(v_j) \\ &= \phi_{i+j}(u_1 \otimes \cdots \otimes u_i \otimes v_1 \otimes \cdots \otimes v_j) \\ &= \phi_{i+j}(a_i b_j). \end{aligned}$$

Proposition 1. Let V be a free R-module with basis $\mathfrak{B} = \{v_j\}$. Then $T(V)$ is a free R-algebra generated by $\mathfrak{B}$.

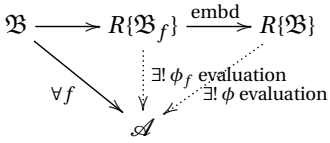
Proof. It follows immediately from the diagram below;



(Lang) Since $V = \bigoplus_I R$, one has $V \otimes V = (\bigoplus_{i\in I} R) \otimes (\bigoplus_{j\in I} R) = \bigoplus_{i,j\in I} R$. Similarly, one has $T^n(V) = \bigoplus_{i_1,\cdots,i_n\in I} R$, so that $\{v_{i_1} \otimes \cdots \otimes v_{i_n} \mid i_1, \cdots, i_n \in I\}$ forms a basis for $T^n(V)$. Now one can assign the suitable values on each basis vectors, nemely, $v_{i_1} \otimes \cdots v_{i_n} \longmapsto f(v_{i_1}) \cdots f(v_{i_n})$. □

Note that this also gives a proof of the existence of a free R-algebra. Indeed this equals to the (non-commutative) polynomial algebra; just regard the basis elements as the indeterminates. For example, $2x^3y^2z = 2x^{\otimes 3} \otimes y^{\otimes 2} \otimes z$. In other words, one can define a non-commutative polynomial algebra as a tensor algebra generated by the indeterminates.

Evaluation homomorphism is well-defiend for each polynimial, since it has only finitely many variables. Let $\mathfrak{B}$ be the set of indeterminates, possibly infinite, and $R\{\mathfrak{B}\}$ be the non-commutative polynomial algebra with $\mathfrak{B}$ as the set of all indeterminates. For a given polynomial f, let $\mathfrak{B}_f$ be the set of all indeterminates that apper in f. Then following commutative diagram



yields the R-evaluation $\phi : R\{\mathfrak{B}\} \to \mathscr{A}$.

Definition 5. A *graded ring* A is a ring that has a direct sum dicomposition into (abelian additive groups)

$$A = \bigoplus_{n\in\mathbb{N}} A_n = A_0 \oplus A_1 \oplus A_2 \oplus \cdots$$

such that for each $x \in A_s$ and $y \in A_r$, it holds that $xy \in A_{s+r}$, and so $A_s A_r \subseteq A_{s+r}$. Elements of A_n are known as *homogeneous elements of degree n*. An algebra $\mathscr{A}$ over a ring R is a *graded algebra* if it is graded as a ring. An ideal or other subset $\mathfrak{a}$ of A is homogeneous if for every element $a \in \mathfrak{a}$, the homogeneous parts of a are also contained in $\mathfrak{a}$.

Example 2. The polynomial rings $k[t] = \bigoplus_{i \in \mathbb{Z}^+} kt^i$ and $k[s,t] = \bigoplus_{i \in \mathbb{Z}^+} \mu_i$ over the field k are graded algebras.

Note 1. There is a natural correspondence between the free R-algebra $\mathscr{F}_{R\text{-alg}}(\mathfrak{B})$ and free commutative R-algebra $\mathscr{F}_{R\text{-comm alg}}(\mathfrak{B})$ generated by $\mathfrak{B}$, namely,

$$\mathscr{F}_{R\text{-alg}}(\mathfrak{B}) / \langle xy - yx \,|\, x, y \in \mathfrak{B} \rangle \approx \mathscr{F}_{R\text{-comm alg}}(\mathfrak{B})$$

To see this, first we need to check that

$$I_1 := \langle xy - yx \,|\, x, y \in \mathfrak{B} \rangle = \langle \alpha\beta - \beta\alpha \,|\, \alpha, \beta \in \mathscr{F}_{R\text{-alg}}(\mathfrak{B}) \rangle.$$

$\subseteq$ is clear, and to show $\supseteq$, it suffices to show for $r_1, r_2 \in R$ and $x, y \in \mathfrak{B}$ that $r_1 x r_2 y - r_2 y r_1 x \in I_1$ by distributivity. Since R is commutative, it amounts to show that $r_1 r_2 (xy - yx) \in I_1$ and this is clear.

Second, isomorphism between the two R-algebras holds in a similar way to the isomorphism between the quotient of a free group modulo the commutator and free abelian group.

Definition 6. Let $\mathscr{S}_0(V) = R$ and define a R-submodule

$$\mathscr{S}^n(V) := \langle (v_1 \otimes \cdots \otimes v_n) - (v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}) \,|\, v_i \in V, \sigma \in S_n \rangle;$$

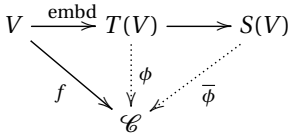
$$\mathscr{S}(V) := \bigoplus_{i \in \mathbb{Z}^i} \mathscr{S}^i(V).$$

Note that $\mathscr{S}(V)$ is a 2-sided ideal of $T(V)$, and hence one can define the *symmetric algebra* $S(V)$on V over the field k by

$$S(V) := T(V) / \mathscr{S}(V).$$

The symmetric algebra $S(V)$ has a graded algebra structure, namely $S(V) = \bigoplus_{n \in \mathbb{Z}^+} S^n(V)$ where $S^n(V) := T^n(V) / \mathscr{S}^n(V)$.
We hope that this symmetric algebra would be a commutative polynomial algebra.

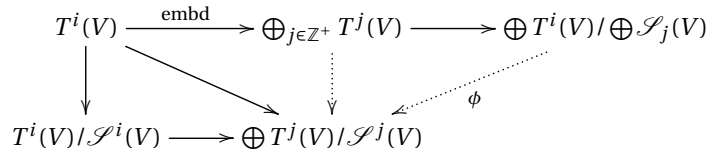
Universal property of symmetric algebra. Let $\mathscr{C}$ be any commutative R-algebra and $f : V \to \mathscr{C}$ be a R-linear map. Then for any R-linear map $V \to \mathscr{C}$, there are unique R-algebra homomorphisms $\phi : T(V) \to \mathscr{C}$ and $\overline{\phi} : S(V) \to \mathscr{C}$ for which the following diagram commutes;



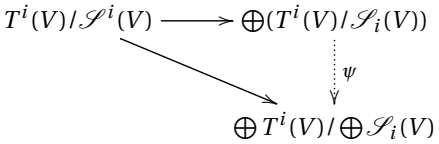
To see this, one needs to check if $\overline{\phi}$ is induced, i.e., $\phi(\mathscr{V}) = 0$. Recall that $\phi = \bigoplus \phi_i$. Then since $\mathscr{C}$ is commutative, we have $f(v_1) \cdots f(v_n) - f(v_{\sigma(1)}) \cdots f(v_{\sigma(n)}) = 0$. Hence $\overline{\phi}$ is induced, and therefore we can say that $S(V)$ is a free commutative R-algebra generated by $\mathfrak{B}$. This is equivalent to say that $S(V)$ is a polynomial algebra with indeterminate set $\mathfrak{B}$.

Proposition 2. $S(V) = T(V)/\mathscr{S}(V) = \bigoplus T^i(V)/\bigoplus \mathscr{S}_i(V) \approx \bigoplus (T^i(V)/\mathscr{S}^i(V))$

Proof. How can we construct the isomorphism $\bigoplus T^i(V)/\bigoplus \mathscr{S}_i(V) \xrightarrow{\approx} \bigoplus (T^i(V)/\mathscr{S}^i(V))$? By the universal property of direct sum and symmetric algebra, there is a R-algebra homomorphism ϕ for which the following diagram is commutative:



For inverse, first note that the map $T^i(V) \to \bigoplus T^i(V)$ induces the map one the quotients $T^i(V)/\mathscr{S}^i(V) \to \bigoplus T^i(V)/\bigoplus \mathscr{S}_i(V)$ since $\mathscr{S}^i(V)$ maps to zero by the embedding. Hence the universal property of direct sum yields that there is a R-algebra homomorphism ψ such that we have the following commutative diagram :



That ψ is the inverse map of ψ comes easily by tracking the basis elements. In the first diagram, we see that ϕ maps a typical basis element $v_1 \otimes \cdots \otimes v_j + \mathscr{S}(V)$ to $v_1 \otimes \cdots \otimes v_j + \mathscr{S}^j(V)$. On the other hand on the second diagram, ψ maps $v_1 \otimes \cdots \otimes v_j + \mathscr{S}^j(V)$ to $v_1 \otimes \cdots \otimes v_j + \mathscr{S}(V)$. This shows $\phi \circ \psi$, $\psi \circ \phi$ are identity maps on the basis elements, and hence they are identity maps on the whole. This shows the desired isomorphism. □

Following proposition corresponds to the observation we made in Note 1.

Proposition 3. $\mathscr{S}(V) = \langle xy - yx \overset{(1)}{|} x, y \in V\rangle = \langle xy - yx \overset{(2)}{|} x, y \in T(V)\rangle$.

Proof. (1) $\subseteq \mathscr{S}(V)$: $xy - yx = x \otimes y - y \otimes x \subset \mathscr{S}(V)$.

(1) $\supseteq \mathscr{S}(V)$: We need to show $v_1 \cdots v_n - v_{\sigma(1)} \cdots v_{\sigma(n)} \in$ (1) where $v_1 \cdots v_n \in T^n(V)$ and $\sigma \in S_n$. Recall that each permutation in S_n is a composition of transpositions. For each $\sigma \in S_n$, let $|\sigma|$ be the smallest number k such that σ can be written by a composition of k transpositions. Let $\tau_1, \cdots, \tau_k$ be a sequence of transpositions such that $\sigma = \tau_k \cdots \tau_1$ and $k = |\sigma|$. Suppose the assertion holds for $|\sigma| < k$. Suppose $\tau_1 = (i, i+1)$. Then we can write

$$\begin{aligned} & (v_1 \cdots v_n) - (v_{\sigma(1)} \cdots v_{\sigma(n)}) \\ = \quad & [v_1 \cdots v_{i-1}(v_i v_{i+1} - v_{i+1} v_i) v_{i+2} \cdots v_n] + \big([v_1 \cdots v_{i-1} v_{i+1} v_i v_{i+2} \cdots v_n] - [v_{\sigma(1)} \cdots v_{\sigma(n)}]\big) \end{aligned}$$

Obviously the first term belongs to (1). Note that the permutation $(1, \cdots, i-1, i+1, i, i+2, \cdots, n) \mapsto (\sigma(1), \cdots, \sigma(n))$ equals $\tau_k \cdots \tau_2$, and hence the remaining term in the large parentheses belongs to (1) by induction hypothesis.

(1) $\subseteq$ (2) : Clear.

(2) ⊆ (1) : (2) ⊆ $\mathscr{S}(V)$ ⊆(1).

□

Definition 7. Let $\mathscr{A} = \bigoplus_{i\in\mathbb{Z}^+} A_i$ be a $\mu-$graded algebra and $\mathfrak{a}$ be a 2-sided ideal of $\mathscr{A}$. Then

$$\begin{aligned}
\mathfrak{a} \text{ is a } \textit{homogeneous ideal} &\iff \mathfrak{a} = \bigoplus_{i\in\mathbb{Z}^+} (\mathfrak{a}\cap A_i) \\
&\iff \text{if } f = \sum_{d\geq 0} f_d \in \mathfrak{a} \text{ then } f_d \in \mathfrak{a} \text{ for all } d, \text{ where each } f_d \text{ is a homogeneous element} \\
&\iff \text{every element of } \mathfrak{a} \text{ is generated by homogeneous elements in } \mathfrak{a}
\end{aligned}$$

HW 2. Show that $\mathfrak{a} \subset \mathscr{A}$ is a homogeneous ideal if and only if it is generated by homogeneous elements.

Example 3. $\langle t^2 - t\rangle \subset \mathbb{R}[t]$ is not a homogenous ideal, whilst $\langle t, t^2\rangle$ is so.

Example 4. In the definition of symmetric algebra $S(V)$ over V, note that $\mathscr{S}(V) = \bigoplus_i \mathscr{S}^i(V)$ is a homogeneous ideal generated by the elements of the form

$$v_1 \otimes \cdots \otimes v_i - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(i)}$$

where $\sigma \in S_i$. According to Proposition 3, it is in fact generated by the homogeneous elements of the form

$$xy - yx, \quad x, y \in V.$$

Graded structure on the symmetric algebra $S(V)$**.** Recall that $S(V) = \bigoplus_{i\in\mathbb{Z}^+} S^i(V)$ where $S^i(V) = T^i(V)/\mathscr{S}^i(V)$: R-module. We want it to be $\mathbb{Z}^+$-graded!

$$\text{multiplication} : S^i(V) \times S^j(V) \to S^{i+j}(V) \quad \text{well-defined?}$$

Let $a_i - a_i' \in \mathscr{S}^i(V)$, $b_j - b_j' \in \mathscr{S}^j(V)$. Then we need to show $a_i b_j - a_i' b_j' \in \mathscr{S}^{i+j}(V)$. Observe that

$$a_i b_j - a_i' b_j' \quad = \quad (a_i - a_i')b_j + a_i'(b_j - b_j')$$

and $(a_i - a_i')b_j$, $a_i'(b_j - b_j') \in \mathscr{S}(V) \cap T^{i+j} = \mathscr{S}^{i+j}(V)$ since $\mathscr{S}(V)$ is homogeneous ideal. Thus the multiplication is well-defined and hence $S(V)$ has a graded ring structure.

Definition 8. The *exterior algebra*(or *alternating algegra*) $\Lambda(V)$ over a vector space V over a field k is defined as the quotient algebra of the tensor algebra by the two-sided ideal I generated by all elements of the form $x \otimes x$ such that $x \in V$. Symbolically,

$$\Lambda(V) := T(V)/I.$$

The exterior product $\wedge$ of two elements of $\Lambda(V)$ is defined by

$$\alpha \wedge \beta = \alpha \otimes \beta \pmod{I}.$$

More explicitely, we may define

$$\begin{aligned}
\Omega_n(V) &:= \langle v_1 \otimes \cdots \otimes v_n \,|\, v_i \in V,\, v_i = v_j \text{ for some } i \neq j\rangle \\
\Omega(V) &:= \bigoplus_{n\in\mathbb{Z}^+} \Omega_n \\
\Lambda^i(V) &:= T^i/\Omega_n(V).
\end{aligned}$$

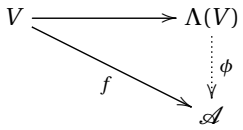
Then one has $\Omega(V) = \langle v \otimes v \,|\, v \in V \rangle = I$, so that

$$\Lambda(V) = \bigoplus_{n \in \mathbb{Z}^+} \Lambda_n(V).$$

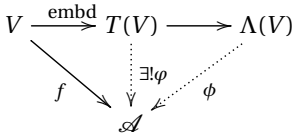
HW 3. Find a suitable example of an exterior algebra.

Definition 9. An R-algebra $\mathscr{A}$ is *algernating algebra* if and only if $a^2 = 0$ for all $a \in \mathscr{A}$.

Universal property of exterior algebra. Let $\mathscr{A}$ be an alternating algebra and let $f : V \to \mathscr{A}$ be a R-linear map such that $f(v)f(v) = 0$ for all $v \in V$. Then there exists a unique R-algebra homomorphism $\phi : \Lambda(V) \to \mathscr{A}$ for which the following diagram commutes;



where the horizontal map is the composition $V \to T(V) \to \Lambda(V) = T(V/I)$ of the quotient map and embedding. This universal property follows from the diagram below;



We only need to check that $\varphi(I) = 0$; indeed, a typical element of I is v^2 for some $v \in V$, and $\varphi(v^2) = \varphi(v)\varphi(v) = f(v)f(v) = 0$.

Proposition 4. Suppose the vector space V has dimension n. Then we have

$$\begin{aligned} \dim T^r(V) &= n^r \\ \dim S^r(V) &= \binom{n+r-1}{r} \\ \dim \Lambda^r(V) &= \binom{n}{r} \end{aligned}$$

Proof. Let $\{v_1, \cdots, v_n\}$ be a basis for V. The first dimensionality is clear. For the second, the dimension equals the number of degree r monomials with n indeterminates. Lastly, the set

$$\{v_{i_1} \wedge \cdots \wedge v_{i_r} \,|\, 1 \le i_1 < i_2 < \cdots < i_r \le n\} \tag{$*$}$$

is a basis for $\lambda^k(V)$. The reason is the following: that the set $(*)$ is k-linearly independent is clear; given any exterior product of the form

$$u_1 \wedge \cdots \wedge u_k$$

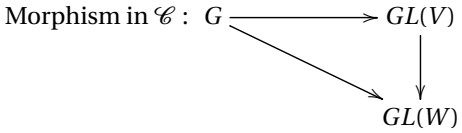
then every vector u_j can be written as a linear combination of the basis vectors v_i; using the bilinearity of the exterior product, this can be expanded to a linear combination of exterior products of those basis vectors.

Any exterior product in which the same basis vector appears more than once is zero; any exterior product in which the basis vectors do not appear in the proper order can be reordered, changing the sign whenever two basis vectors change places; consequently $(*)$ spans $\lambda^k(V)$. In general, the resulting coefficients of the basis k-vectors can be computed as the minors of the matrix that describes the vectors u_j in terms of the basis v_i. □

2 Representation Theory

Definition 10. Let V be a k-vector space. A group homomorphism $\phi : G \to GL(V)$ is called a representation of G over V. An injective representation is called *faithful*.

Let $\mathscr{C}$ be the category of [representations of G over k-vector space].



Note that $\mathscr{C}$ is isomorphic to the category of $k[G]$-modules $\mathrm{Mod}(k[G])$. Hence the study of representation is equivalent to study $k[G]$-modules.

Definition 11. A R-module is *irreducible* or *simple* if it has no nonzero proper submodules.

Simple modules are analogous to the simple groups in group theory.

Proposition 5 (Lang p.645)**.** Let R be a ring not necessarily being commutative. Let E be a R-module. These followings are equivalent.

(1) $E = \sum_i E_i$, where E_i is irreducible(simple) R-module.

(2) $E = \bigoplus_j F_j$ where F_i irreducible(simple) R-module.

(3) For any R-submodule $F \leq_R E$, there exists $F' \leq_R E$ such that $E = F \oplus F'$.

Proof. (1) $\Rightarrow$ (2). Assume (1). I claim that there exists a subset $J \subset I$ such that E is the direct sum $\bigoplus_{j\in J} E_j$. To see this, let J be a maximal subset of I such that the sum $\sum_{j\in J} E_j$ is direct(by Zorn's Lemma). We contend that is sum is in fact equal to E. It will suffice to show that each E_i is contained in this sum. But the intersection of our sum with E_i is a submodule of E_i, hence equal to 0 or E_i. If it is equal to 0, then one can add the index i to J, which contradicts the maximality of J. Hence the intersection equals to E_i and thus $E_i \subset \sum_{j\in J} E_j$. This show the claim. This also shows the implication (1) $\Rightarrow$ (2).

(2) $\Rightarrow$ (3). Assume (2). We may assume $F \neq 0$, since otherwise we can take $F' = E$. Since $E_i \cap F \leq_R E_i$ and E_i is simple, either $E_i \cap F = 0$ or $E_i \leq_R F$. Since F is nonzero, there is some E_i contained in F. Now let J be the maximal subset of I such that $\bigoplus_J E_j \subseteq F$(by Zorn's Lemma). If the inclusion is proper, then there is some $i \in I \setminus J$ such that $E_i \cap F \neq 0$; but this means $E_i \subset F$, and hence we get a larger index set $J \cap \{i\} \subset I$ which contradicts our choice of J. Thus $\bigoplus_J E_j = F$. Now take $F' = \bigoplus_{I\setminus J} E_i$.

(3) $\Rightarrow$ (1). Assume (3). I claim that every nonzero submodule E' of E contains a simple submodule. Let $v \in E'$, $v \neq 0$. Then by definition, Rv is a principal submodule, and the kernel of the homomorphism

$$R \to Rv$$

is a left ideal $L \neq R$. Hence L is contained in a maximal ideal $M \neq R$(by Zorn's Lemma). Then M/L is a maximal ideal of R/L, and hence Mv is a maximal submodule of Rv, corresponding to M/L under the isomorphism

$$R/L \to Rv.$$

By (3), we can write $E = Mv \oplus M'$ for some submodule M' of E. Then we have

$$Rv = Mv \oplus (M' \cap Rv),$$

since every element $x \in E'$ can be written uniquely as a sum $x = \alpha v + x'$ with $\alpha \in M$ and $x' \in M$, and $x' = x - \alpha v$ lies in Rv. Then since Mv is maximal in Rv, it follows that $M' \cap Rv$ is simple, as desired.(otherwise there would be a nonzero proper submodule S of $M' \cap Rv$, to form a proper submodule $Mv+S$ of $M' \cap Rv$ properly containing the maximal one Mv, which is a contradiction.) This proves the claim.

We now show (3) imples (1). Let E_0 be the sum of all simple submodules of E. We may assume $E_0 \neq E$ for contradiction. Then there exists a nonzero submodule $F \leq_R E$ such that $E = E_0 \oplus F$. Then by the claim, F contains a simple submodule $F' \leq_R E$. But then $F' \subset E_0$ by the choice of E_0, which is a contradiction. Thus $E = E_0$.

□

We call such a R-module a *semisimple R-module* or *completely reducible R-module*.

Example 5. Any vector space over the field k is a semisimple k-module. The simple k-modules are 1-dimensional subspaces, and for any given subspace, we can obtain the complimentary space by basis extension.

Proposition 6. Let E be a semisimple R-module. Show that a submodule and quotient of E is also semisimple.

Proof. Suppose $E' \leq_R E$ and let F be any submodule of E'. Since E is semisimple, we have $E = F \oplus F'$. Then it follows by taking intersection with E' that $E' = F \oplus (F' \cap E)$. Hence E' is semisimple. As for the quotient module, say E/F, we may write $E = F \oplus F'$ for some $F' \leq_R E$. Then the cannonical projection $E \to E/F$ induces an isomorphism of F' onto E/F. Hence E/F is semisimple being isomorphic to a submodule of E. □

Definition 12 (Lang p.651)**.** A ring R is a *semisimple ring* if ${}_RR$ is a semisimple R-module.

Proposition 7. Let R be a semisimple ring. Then every R-module E is a semisimple R-module.

Proof. First observe that every free R-module F is semisimple; since we have $F \simeq \bigoplus_I {}_RR$, and R is a semisimple ring, F is a direct sum of semisimple R-modules. Then since each of the factor module ${}_RR$ is a direct sum of simple R-modules, F is also a direct sum of simple R-modules. Hence F is semisimple. Now since E is a quotient module of a free R-module and a quotient module of a semisimple R-module is semisimple, we conclude that E is also semisimple. □

Example 6 (Lang p.651)**.** Examples of semisimple ring.

(1) $R = k$.

(2) The algebra $\mathfrak{M}_{n,n}(k)$ of $n \times n$ matrices over k.

(3) Group algebra $k[G]$ where $|G| < \infty$ and $\mathrm{char}(k) \nmid |G|$.

(4) The Clifford algebras C_n over the real numbers.

By definition the group algebra $k[G]$ is a k-vector space with k-basis G. Multiplication on the basis elements is given by the binary operation in G. Following theorem of Maschke explains the third item of the above example.

Theorem 1 (Maschke)**.** $|G| < \infty$ and $\mathrm{char}(k) \nmid |G| \Longrightarrow k[G]$: semisimple ring.

Proof. (Special case) Suppose k is a subfield of $\mathbb{R}$ and V be a finite dimensional $k[G]$-module. We want to show

$$W \leq_{k[G]} V \Longrightarrow \exists W' \leq_{k[G]} V \text{ such that } V = W \oplus W'.$$

Want : $V = W \oplus W^{\perp}$. Let $\{v_i\}$ be a basis for V and define dot product by $\langle v_i, v_j \rangle = \delta_{ij}$. But in order for $W^{\perp} \leq_{k[G]} V$, we want G-invariant inner product since then we would have for every $v \in W^{\perp}$ and $g \in G$,

$$\langle gv, W \rangle = \langle g^{-1}gv, g^{-1}W \rangle = \langle v, g^{-1}W \rangle = \langle v, W \rangle = 0 \quad \Longrightarrow gv \in W^{\perp}.$$

Such a G-invariant inner product on V can be defined by

$$v \bullet w = \sum_{g \in G} \langle gv, gw \rangle.$$

Note that this inner product is positive definite.

(General case) Let $W \leq_{k[G]} V$. Since $W \leq_k V$, there is a k-subspace $W' \leq_k V$ such that $V = W \oplus W'$(basis extension). Let $\pi : V \to W$ be the cannonical projection. Now we want to show following short exact sequence of $k[G]$-modules is split;

$$0 \longrightarrow W \xrightarrow{i} V \longrightarrow V/W \longrightarrow 0,$$

for which it suffices to show there is a $k[G]$-linear map $\phi : V \to W$ such that $\phi \circ i = id_W$. Let us define a map $\phi : V \to W$ by

$$\phi(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gv) \quad (\mathrm{char}(k) \nmid |G|\,), \tag{$*$}$$

The property $\phi \circ i = id_W$ is immediate $W \leq_{k[G]} V$ and π is identity on W, and clearly ϕ is k-linaer. In fact, it is $k[G]$-linear; for $h, v \in G$, we have

$$\begin{aligned} \phi(hv) &= \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(ghv) \\ &= \frac{1}{|G|} \sum_{t \in G} ht^{-1}\pi(tv) \qquad (t = gh) \\ &= \frac{h}{|G|} \sum_{t \in G} t^{-1}\pi(tv) = h\phi(v). \end{aligned}$$

Therefore $V = W \oplus \ker\phi$ where $\ker\phi \leq_{k[G]} V$

□

Note that the definition $(*)$ is motivated by Haar measure of Locally compart group.
Due to Maschke's Theorem, the study of simple $k[G]$-module is equivalent to the study of the (linear) representation of G over the field k, provided that the hypothesis of the theorem is satisfied. We are not so interested in the exceptional cases.

Representation of S_3
$S_3 = \{1, \sigma, \tau, \sigma\tau, \sigma\tau^2, \tau^2\}$, $\sigma^2 = \tau^3 = 1$, $\sigma\tau\sigma = \tau^2$

Maschke + Wedderburn + α.

Theorem 2. $|G| \leq \infty$, $\mathrm{char}(k) \nmid |G| \Rightarrow k[G]$: semisimple. Let k be algebraically closed. Then

$$k[G] \overset{R\text{-alg}}{\approx} \mathrm{End}_k(V_1) \times \cdots \times \mathrm{End}_k(V_r)$$

where $\{V_1, \cdots, V_r\}$ is the complete list of irreducible representations of G over k(up to equivalence)

Proof. Omitted. □

$\mathrm{Mor}(G \to GL(V), G \to GL(W)) = \mathrm{Mor}_{k[G]}(GL(V), GL(W))$.

Corollary 1. If we put $n_i := \dim_k(V_i) < \infty$, then we have

$$|G| = \dim_k(k[G]) = n_1^2 + \cdots + n_r^2.$$

Recall that $[g] = \{hgh^{-1} \mid h \in G\}$.

Corollary 2. Moreover, r is the number of conjugacy classes of G.

Proof. Observe that $r = \dim_k(Z(k[G]))$; center of product algebra is the product of the centers, and the center of a matrix algebra is 1-dimensional.
On the other hand, let $C_1, \cdots, C_s$ be the list of all conjugacy classes of G. Put $z_i = \sum_{g \in C_i} 1 \cdot g$. We claim that $\mathfrak{B} = \{z_1, \cdots, z_s\}$ is a k-basis of $Z(k[G])$. It is clear that $\mathfrak{B} \subset Z(k[G])$; for any $h \in G$, $hz_ih^{-1} = \sum_{g \in C_i} 1 \cdot hgh^{-1} = z_i$ since the conjugation by h fixes the conjugacy class C_i. To show $\mathfrak{B}$ spans $Z(k[G])$, put $\sum_{g \in G} a_g \cdot g \in Z(k(G))$ where $a_g \in k$. Then

$$\begin{aligned} h(\sum_g a_g \cdot g)h^{-1} &= \sum_g a_g hgh^{-1} \\ &= \sum_g a_{hgh^{-1}} g = \sum_g a_g \cdot g \end{aligned}$$

and since the elements of G forms a basis for the k-vector space $k[G]$, we see that $a_g = a_{hgh^{-1}}$ for all g. This shows $\mathfrak{B}$ spans $Z(k[G])$, and proves the claim. Now we conclude $r = s$ as desired. □

Example 7. $G \approx \mathbb{Z}_3$. $3 = \sum n_i^2 = 1+1+1$. Since $\mathbb{Z}_3$ is abelian, the conjugacy classes are just the single elements; hence $r = \#$ of conjugacy classes $= 3$.
$G \to k^\times = GL_1(k)$ group homomorphism, $x \mapsto w$ where $w^3 = 1$.

Definition 13. Group character.

(1) Group homomorphism $G \to k^\times$

(2) Group homomorphism $\phi : G \to GL(V)$, $\dim V < \infty$.

$$\chi(g) = \mathrm{tr}(\phi(g)).$$

Example 8. $G \approx \mathbb{Z}_5$. $5 = \sum n_i^2 = 1+1+1+1+1 = 1+2^2$.

Example 9. $G \approx \mathbb{Z}_4$. Since every group has the trivial representation which is 1-dimensional, namely $G \to GL_1(k) = k^\times$ by $g \mapsto 1$, we have $4 = \sum n_i^2 = 1+1+1+1$.

Example 10. $G \approx \mathbb{S}_3$. $[1] = 1$, $[\tau] = \{\tau, \tau^2\}$, $[\sigma] = \{\sigma, \sigma\tau, \sigma\tau^2\}$.$(\tau\sigma\tau^{-1} = \sigma\tau^2\sigma^{-1} = \sigma\tau)$. Hence $r = 3$, and $6 = 1+1+4$.

(1) trivial representation : $S_3 \to \{1\} \subset k^\times$

(2) sgn : $S_3 \to \{\pm 1\} \subset k^\times$

(3) $\Psi_1 : S_3 \to GL_2(k)$, where $\sigma \mapsto \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\tau \mapsto R_{2\pi/3}$ ····· rigid motion.

(4) $\Psi_2 : S_3 \to GL_2(k)$, where $\sigma \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\tau \mapsto \begin{bmatrix} \zeta & 0 \\ 0 & \zeta \end{bmatrix}$ where $1 + \zeta + \zeta^2 = 0$.

Example 11. $|G| = 8 = 1+1+1+1+4 = 1+1+1+1+1+1+1+1$. Note that if every irreducible representation is 1-dimensional, then G is abelian.(need to prove). Hence if we assume G non-abelian, then $|G| = 1+1+1+1+4$.

Even if we have found a representation $\phi : G \to GL(V)$, we might not be able to fined a basis of V. So matrix representation is hard. In this case, we use *character table*

Theorem 3 (Burnside)**.** Let p, q be prime integers and a, b be positive integers. Then every group of order $p^a q^b$ is solvable.

Proof. Use Character theory. □

Topological Group

Definition 14. A group G is a topological group if it satisfies following properties:

(i) G is a topological space

(ii) $* : G \times G \to$, inverse : $G \to G$ are continuous maps, where we give product topology to $G \times G$.

HW 4. Show that $(\mathbb{R}, +)$, $(\mathbb{R}^\times, \times)$ are topological groups.

Proposition 8. Let G be a topological group and $g \in G$. Then the neighborhood of g is homeomorphic to the neighborhood of e.

Proof. $e \in U \to gU$ homeomorphism. □

3 Inverse Limits

Definition 15. I is a *directed index set* if

(i) : I is a poset

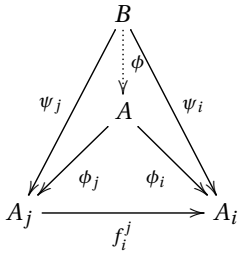
(ii) : If $i, j \in I$, then there is $k \in I$ such that $i \leq k$ and $j \leq k$.

Definition 16. Let $\mathscr{C}$ be a category, and I a directed set. We call $A = \{A_i, f_i^j\}$ a *directed system* if $A_i \in \mathscr{C}$ and $f_i^j : A_j \to A_i$ for all $i \leq j$ such that

(i) : $f_i^i = id$

(ii) : $i \leq j \leq k \Rightarrow f_i^j \circ f_j^k = f_i^k$.

The inverse limit $A := \varprojlim_{i \in I} A_i$ is defined by the following universal property(think of the product $\prod_i A_i$) : for any $B \in \mathscr{C}$ and morphisms $\psi_j : B \to A_j$ and $\psi_i : B \to A_i$ such that $f_i^j \circ \psi_j = \psi_i$, there exists unique morphism $\phi : B \to A$ such that following diagram commutes



Example 12. Let X be a topological space. Let U be an open subset. Then $C_U := \{f : U \to \mathbb{R} \mid \text{continuous}\}$ is an abelian group. Restriction is a typical example.

Example 13. Let X be a set, and $\mathscr{P}$ a subset of the power set $P(X)$. Assume $\mathscr{P}$ is a directed set with respect to the inverse set inclusion. We define $f_B^A \to : A \to B$ inclusion for each $A \leq B$(i.e., $A \subset B$).

Example 14. Let k be a field. The power series ring $k[[T]]$ in one variable may be viewed as the inverse limit of the factor polynomial rings $k[T]/(T^n)$, where for $n \leq m$ we have the cannonical ring homomorhism

$$f_m^n : k[T]/(T^n) \longrightarrow k[T]/(T^m).$$

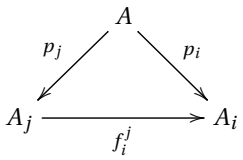
A similar remark applies to power series in several variables.

Example 15. Let p be a prime integer, and suppose $1 \leq n \leq m$. There is a natural map $f_n^m : \mathbb{Z}/(p^{m+1}) \to \mathbb{Z}/(p^{n+1})$. We call the inverse limit of $\mathbb{Z}/(p^m)$ *the ring of p-adic integers* and denote $\mathbb{Z}_p$.

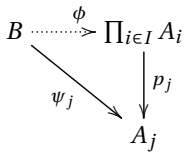
Theorem 4. Suppose the Cartesian product and categorical product in $\mathscr{C}$ agree. Then we have

$$\varprojlim_{i \in I} A_i = \left\{ \mathbf{x} \in \prod_{i \in I} A_i \;\middle|\; f_i^j(\mathbf{x}(j)) = \mathbf{x}(i) \quad \forall i \leq j \right\}$$

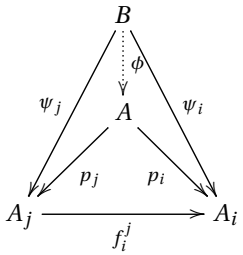
Proof. Let A be the subset of the Cartesian product on the right hand side of the assertion. Note that A is maximal subset of $\prod_i A_i$ such that the following diagram is commutative:



Given $B \in \mathscr{C}$ and morphisms $\psi_j : B \to A_j$, the universal property of the categorical product yields that we get a unique morphism $\phi : B \to \prod_{i\in I} A_i$ such that the following diagram commutes;



Now it remains to check if ϕ is *into* A, since then we would obtain the desired commutative diagram



Indeed, for any $b \in B$ we have

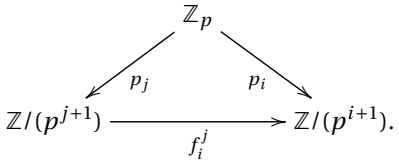
$$f_i^j \, p_j(\phi(b)) = f_i^j \circ (p_j \circ \phi)(b) = f_i^j \circ \psi_j(b) = \psi_i(b) = p_i(\phi(b)).$$

so that $\phi(b) \in A$. This shows A satisfies the universal property of the inverse limit $\varprojlim_{i\in I} A_i$. □

Example 16. By the above theorem, we see that the ring $\mathbb{Z}_p$ of p-adic integers is given by

$$\mathbb{Z}_p = \left\{ (x_0, x_1, x_2, \cdots) \in \prod_{i\in\mathbb{Z}^+} \mathbb{Z}/(p^i) \mid x_n \equiv x_{n-1} \pmod{p^n} \right\}$$

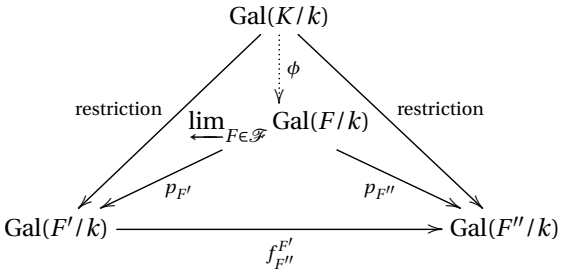
by considering the diagram



Example 17. We can describe the Galois group of even an infinite Galois extension as an inverse limit of finite Galois groups. Let K/k be a Galois extension, not necessarily finite. Consider a tower $k \leq F \leq K$. Denote $G = \mathrm{Gal}(K/k)$ and $H = \mathrm{Gal}(K/F)$. Recall that K/F is automatically Galois, and F/k is finite Galois if and only if $H \lhd G$ and $[G : H] < \infty$. Now we form a directed system of finite Galois groups of finite Galois extensions F/k such that $k \leq F \leq K$ in following way: the intermediate fields $k \leq F \leq G$ forms the directed index set $\mathscr{F}$, and for the tower $k \leq F \leq F' \leq K$, we define $f_{F'}^{F'} : \mathrm{Gal}(F'/k) \to \mathrm{Gal}(F/k)$ by the restriction map. Now consider the inverse limit of this directed system. Since the catetorical and Cartesian product agrees in the category of groups, we see that

$$\varprojlim_{F \in \mathscr{F}} \mathrm{Gal}(F/k) \leq \prod_{F \in \mathscr{F}} \mathrm{Gal}(F/k).$$

Let p_F be the projection from the inverse limit onto the Galois group $textGal(F/k)$ for each $F \in \mathscr{F}$. Then one can show that there is a natural homomorphism ϕ from the Galois group $\mathrm{Gal}(K/k)$ to the inverse limit, such that the following diagram commutes:



But by the universal property of the inverse limit, we conclude that ϕ is an isomorphism. For details, we need to define Krull topology on the automorphism group $\mathrm{Gal}(K/k)$. Analogous to the Galois correspondence of finite Galois theory, we have the 1:1 correspondence between closed subgroups of $\mathrm{Gal}(K/k)$with the (arbitrary) intermediate fields.

Definition 17. Inverse limit of finite groups is called *profinite group*. Inverse limit of cycle group is called *procyclic group*.

Example 18. Let each G_i has dicrete topology and suppose $1 < |G_i| < \infty$. The product $\prod_{\in I} G_i$ is not necessarily discrete. But it is at least *totally disconnected*(the only connected components are the empty set and point sets) An important example of a totally disconnected space is the Cantor set. Another example, playing a key role in algebraic number theory, is the field $\mathbb{Q}_p$ of p-adic numbers.

HW 5. Let $\{G_i, f_i^j\}$ be a discrete system where each G_i is a compact discrete space. Show the inverse limit of G_i is totally disconnected and compact.

The ring of p-adic inters is totally disconnected and compact. A p-adic integer looks like $(a_0, a_1, \cdots)$, where for each n it satisfies $a_n \equiv a_{n-1} (\mathrm{mod}\ p^n)$ since $a_k \in \mathbb{Z}/p^{k+1}$. It equals another p-adic number $(b_0, b_1, \cdots)$ iff $a_i \equiv b_i (\mathrm{mod}\ p^{i+1})$

Example 19. $p = 7$. $(3, 10, 3 + 7 \cdot 1 + 7^2 \cdot 2, \cdots)$

4 ABSOLUTE VALUE AND VALUATION

Minkovski's Motivation. Consider $x_0^2 \equiv 2(\text{mod}7)$, which has solution $x_0 = 3$ or 4. Also consider $x_1^2 \equiv 2(\text{mod } 7^2)$. Regard a number is "small" if it can be divided by a large power of prime p.

Definition 18. Let k be a field. Then $|\cdot| : k \to \mathbb{R}^{\geq 0}$ is an *absolute value* if

(i) (nondegenerate) $|\alpha| > 0$ if $\alpha \neq 0$ and $|0| = 0$

(ii) (multiplicative) $|\alpha\beta| = |\alpha| \cdot |\beta|$

(iii) (triangle inequality) $|\alpha + \beta| \leq |\alpha| + |\beta|$

An absolute value with

$$\text{(iii)'} \quad |\alpha + \beta| \leq \max(|\alpha|, |\beta|)$$

is called a *valuation*(non-archimedian).

Example 20. Let p be a fixed prime in 2. If $a \neq 0$ in $\mathbb{Q}$, we write $a = p^k \frac{b}{c}$ where $k \in \mathbb{Z}$ and $(b, p) = 1 = (c, p)$. The integer k is uniquely determined by a. We denote it as $v_p(a)$ and we define $v_p(0) = \infty$. Now let γ be a real number such that $0 < \gamma < 1$ and define a *p-adic absolute value* $|a|_p$ on $\mathbb{Q}$ by

$$|a|_p = \gamma^k.$$

Example 21. Let k(x) be the field of rational expressions in an indeterminate x and let $p(x)$ be a prime polynomial in $k(x)$. If $a \in k(x)$ and $a \neq 0$, we have $a = p(x)^k b(x)/c(x)$ where $k \in \mathbb{Z}$ and $(p(x), b(x)) = 1 = (p(x), c(x))$. We define $v_p(a) = k$, $v_p(0) = \infty$. Then for some real γ, $0 < \gamma < 1$, we have an absolute value on $k(x)$ defined by

$$|a|_p = \gamma^{v_p(a)}.$$

Example 22. We obtain another absolute value on $k(x)$ in the following manner. If $a \neq 0$, we write $a = b(x)/c(x)$ where $b(x) = b_0 + b_1 x + \cdots + b_m x^m$, $c(x) = c_0 + c_1 x + \cdots + c_n x^n$, $b_i, c_i \in k$, $b_m, c_m \neq 0$. Define $v_\infty(a) = n - m$, $v_\infty(0) = 0$, and $|a|_\infty = \gamma^{v_\infty(a)}$ where $\gamma \in \mathbb{R}$ and $0 < \gamma < 1$. Then we have

$$\begin{aligned} a &= \frac{x^m(b_0 x^{-m} + b_1 x^{-(m-1)} + \cdots + b_m)}{x^n(c_0 x^{-n} + c_1 x^{-(n-1)} + \cdots + c_n} \\ &= \frac{(b_0 x^{-m} + b_1 x^{-(m-1)} + \cdots + b_m)}{(c_0 x^{-n} + c_1 x^{-(n-1)} + \cdots + c_n} x^{-(n-m)}. \end{aligned}$$

Hence the definition of $|a|_\infty$ amounts to using the generator x^{-1} for $F(x)$ and applying the procedure in example 2 to $k[x^{-1}]$ with $p(x^{-1}) = x^{-1}$. Hence $|\cdot|_\infty$ is an absolute value on $k(x)$. In the special case of $k = \mathbb{C}$, $v_\infty(a)$ gives the behaviour at ∞ of the rational function defined by a.

For any field k we have the *trivial* absolute value on k in which $|0| = 0$ and $|a| = 1$ if $a \neq 0$.
Below are a list of simple properties of absolute values that follow directly from the definition:

$$|1| = 1, \qquad |u| = 1 \text{ if } u^n = 1, \qquad |-a| = |a|, \qquad |a^{-1}| = |a|^{-1} \text{ if } a \neq 0, \qquad ||a| - |b||_\infty \leq |a - b|.$$

An absolute value on k defines a metric topology on k. It is easy to check that the multiplication, addition, and subtraction are continuous maps of two variables in the topology. We can also define convergence of

sequences and series in the usual way. Thus we may say that $\{a_n | n = 1,2,\cdots\}$ *converges* to a if for every real $\epsilon > 0$, there exists an integer $N = N(\epsilon)$ such that

$$|a - a_n| < \epsilon$$

for all $n \geq N$. In this case we also write $\lim a_n = a$ or $a_n \to a$.

Definition 19. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on k are *equivalent* if they define the same topology on k.

Example 23. If $|\cdot|_p$ and $|\cdot|'_p$ are p-adic valuations defined by γ and γ' respectively, that is, $|a|_p = \gamma^{v_p(a)}$ and $|a|'_p = \gamma'^{v_p(a)}$, then $|a|'_p = |a|_p^s$ for $s = \log\gamma'/\log\gamma > 0$. Hence the spherical neighborhood of a point defined by one of these absolute values is a spherical neighborhood defined by the other. Thus $|\cdot|_p$ and $|\cdot|'_p$ defines the same tolopogy. Note that this is the case for any field k and any two absolute values $|\cdot|$ and $|\cdot|' = |\cdot|^s$ for some $s > 0$.

Remark 1. The topology of k defined by an absolute value $|\cdot|$ is discrete if and only if $||$ is trivial. It is clear that the trivial absolute value defines the discrete topology. Conversely, if $|\cdot|$ is not trivial, then there is some $a \in k$ such that $0 < |a| < 1$. Then $a^n \to 0$ and the set of points $\{a^n\}$ is not closed in k, so the topology is not discrete.

It is now clear that the only absolute value equivalent to the discrete one $|\cdot|$ is $||$ itself. For nontrivial absolute values we shall now show that equivalence can hold only if each absolute value is a positive power of the other.

Theorem 5. Let $|\cdot|_1$ and $|\cdot|_2$ be absolute values of a field k such that $|\cdot|_1$ is not trivial and the unit open ball in $|\cdot|_1$ is contained in the unit open ball in $|\cdot|_2$, i.e.,

$$\{a \in k \,|\, |\alpha|_1 < 1\} \subset \{a \in k \,|\, |\alpha|_2 < 1\}.$$

Then there exists a positive real number s such that $|\cdot|_2 = |\cdot|_1^s$(that is, $|a|_2 = |a|_1^s$ for all $a \neq 0$). Hence $|\cdot|_1$ and $|\cdot|_2$ are equivalent.

Proof. See Jacobson 2 p.541. □

Theorem 6. An absolute value $|\cdot|$ of a field k is non-archimedean if and only if $|n \cdot 1| \leq 1$ for all $n \in \mathbb{Z}$.

Proof. (Artin) If $|\cdot|$ is non-archimedean, then $|n \cdot 1| = |1 + \cdots + 1| \leq |1| = 1$ for all $n \in \mathbb{Z}$. Conversely, suppose this tholds and let $a, b \in k$. Then for any positive integer n we have

$$\begin{aligned} |a+b|^n &= \left| a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + b^n \right| \\ &\leq |a^n| + |a^{n-1}||b| + \cdots + |b^n| \\ &\leq (n+1)\max(|a^n|, |b^n|). \end{aligned}$$

Hence we obtain $|a+b| \leq (n+1)^{\frac{1}{n}} \max(|a|,|b|)$. Since $(n+1)^{\frac{1}{n}} \to 0$ in $\mathbb{R}$, this yields $|a+b| \leq \max(|a|,|b|)$. □

Corollary 3. Any absolute value on a field of characteristic $p \neq 0$ is non-archimedean.

Proof. Let n be an integer. If $n \cdot 1 \in k$ and $n \cdot 1 \neq 0$, then $(n \cdot 1)^{p-1} = \frac{1}{n \cdot 1}(n \cdot 1)^p = \frac{1}{n \cdot 1} n \cdot 1 = 1$. Thus $|n \cdot 1| = 1$, and also $|0| = 0$. Hence $|\cdot|$ is non-archimedean by the Theorem 6. □

The trivial absolute value is non-archimedean. It is clear also from Theorem 6 that if $|\cdot|$ is non-archimedean on a subfield of a field k, then $|\cdot|$ is non-archimedean on k. Hence we have

Corollary 4. If $|\cdot|$ is trivial on a subfield, then $|\cdot|$ is non-archimedean.

Exercise 2. Show that

(1) if $|\cdot|$ is an absolute value and let $0 < s < 1$ be a real number, then $|\cdot|^s$ is an absolute value.

(2) if $|\cdot|$ is a valuation, then $|\cdot|^s$ is an absolute value for every $s > 0$.

Proof. (1) The nondegeneracy and multiplicativity are clear. For triangle inequality, we may assume $a, b \in k$ nonzero and show $|a+b|^s \leq |a|^s + |b|^s$. Note that

$$(1+x)^s \leq (1+x^s)$$

for all $x \leq 0$. To see this, set $f(x) = 1 + x^s - (1+x)^s$ and observe $f(0) = 0$ and $f'(x) = s(x^{s-1} - (1+x)^{s-1}) \geq 0$ for $x \geq 0$ and $0 < s < 1$. Now put $x = |b|/|a|$ and multiply both side by $|a|^s$ to obtain the desired inequality.

(2) It suffices to show the triangle inequality. For $a, b \in k$, observe that $|a+b| \leq \max(|a|, |b|)$ yields $|a+b|^s \leq \max(|a|^s, |b|^s) \leq |a|^s + |b|^s$.

□

Exercise 3. Show that if $|\cdot|$ is non-archimedean, then $|a+b| = |a|$ if $|a| > |b|$. Show also that if $a_1 + \cdots + a_n = 0$, then $|a_i| = |a_j|$ for some $i \neq j$.

Proof. Since $|\cdot|$ is non-archimedean we have $|a+b| \leq |a|$. On the other hand, since $a = (a+b) - b$, we also have $|a| \leq \max(|a+b|, |b|)$. But since $|a| > |b|$, we see that $|a| \leq |a+b|$. This shows $|a+b| = |a|$. We can generalize this statement as follows; $|a_1 + \cdots + a_n| = |a_1|$ if $|a_1| > max(|a_2|, \cdots, |a_n|)$. To see this, just apply the previous statement to $a_1 + b$ where $b = a_2 + \cdots + b_n$. By assumption $|a_1| > |b|$ and hence $|a_1 + b| = |a_1|$.
For the second assertion, suppose for contrary that all the real numbers $|a_1|, \cdots, |a_n|$ are distinct. We may assume $|a_1|$ is the greatest. Then $-a_1 = a_2 + \cdots + a_n$ yields

$$|a_1| = |a_2 + \cdots + a_n| = \max(|a_2|, \cdots, |a_n|) < |a_1|,$$

which is a contradiction. This shows the second assertion. □

Exercise 4. Let $|\cdot|$ be an absolute value on E and assume that $|\cdot|$ is trivial on a subfield k such that E/k is algebraic. Show that $|\cdot|$ is trivial on E.

Proof. Suppose for contrary that there is an element $a \in k$ such that $|a| < 1$. Since a is algebraic over k, there are $c_0, \cdots, c_m \in k$ with $c_m, c_0 \neq 0$ such that $c_m a^m + \cdots + c_1 a + c_0 = 0$. Since $|\cdot|$ is trivial on k by hypothesis, we have

$$|a||c_m a^{m-1} + \cdots + c_1| = |c_0| = 1,$$

which yields

$$|c_m a^{m-1} + \cdots + c_1| = |a|^{-1} > 1.$$

On the other hand, since $|\cdot|$ is non-archimedean by Corollary 4, we get

$$|c_m a^{m-1} + \cdots + c_1| \leq \max(a^m, \cdots, 1) = 1,$$

which is a contradiction. Therefore $|\cdot|$ is trivial on E. □

Example 24. (1) $\{\alpha \in \mathbb{Q} \,|\, |\alpha|_p < 1\} = \{\frac{pb}{a} \,|\, a \neq 0,\ p \nmid a\}$

(2) $\{\alpha \in \mathbb{Q} \,|\, |\alpha|_p \leq 1\} = \{\frac{b}{a} \,|\, a \neq 0,\ p \nmid a\} = \mathbb{Z}_{(p)} S^{-1}\mathbb{Z}\}$ where $S = \mathbb{Z} - (p)$
: local ring with maximal ideal $\{\alpha \in \mathbb{Q} \,|\, |\alpha|_p < 1\}$.

Note that if $|\cdot|$ is a valuation on a field k, then $\{\alpha \in k \,|\, |\alpha| \leq 1\}$ is a ring since for any element α, β of it we have

$$|\alpha + \beta| \leq \max(|\alpha|, |\beta|) \leq 1 \qquad |\alpha\beta| = |\alpha| \cdot |\beta| \leq 1$$

This ring is called *the valuation ring.*

Proposition 9. The only non-trivial absolute value on $\mathbb{Q}$ up to equivalence is

(1) Euclidean absolute value if archimedean

(2) p-adic valuation on $\mathbb{Q}$ if non-archimedean

Proof. (1) See Jacobson 2, p.545.

(2) Let $|\cdot|$ be a non-archimedean absolute value on $\mathbb{Q}$. Then we have $|n| \leq 1$ for every integer n. If $|n| = 1$ for all n, then $|\cdot|$ is trivial, contrary to the hypothesis. Hence there is some nonzero integer n such that $0 < |n| < 1$. Hence the set $P \subset \mathbb{Q}$ of all integers b such that $|b| < 1$ contains nonzero element. It is easy to see that P forms an ideal in $\mathbb{Z}$, since for any $a, b \in P$ and $c \in \mathbb{Z}$ we have $|a + b| \leq \max(|a|, |b|) < 1$ and $|ca| = |c||a| < 1$. Moreoer, P is a prime ideal since $|n| = |n'| = 1$ implies $|nn'| = 1$. Hence $P = (p)$ for some prime integer p. Now let $\gamma = |p|$ so that $0 < \gamma < 1$. Now let $r \in \mathbb{Q}$ be arbitrary. Write $r = p^k \frac{a}{b}$ for some $k, a, b \in \mathbb{Z}$ such that $a, b \notin (p)$. This means $|a| = |b| = 1$, and hence $|r| = |p^k| = \gamma^k = \gamma^{v_p(r)}$. Hence $|\cdot|$ is the p-adic absolute value defined by γ.

□

Proposition 10. Let $|\cdot|$ be a non-trivial absolute value on $k(x)$, x trancendental, that is trivial on k. Then $|\cdot|$ is one of the absolute values defined in Example 20 and 21.

Proof. Case I. $|x| \leq 1$: In this case, the fact that $|\cdot|$ is trivial on k and non-archimedean implies that $|f| \leq 1$ for all $f \in k(x)$. Since $|\cdot|$ is not trivial, there should be some nonzero element $b \in k(x)$ such that $0 < |b| < 1$. Hence the set $P \subset k[x]$ of all elements c with $|c| < 1$ contains nonzero element. Then P forms an ideal in $k[x]$; for any $a, b \in P$ and $c \in k[x]$, we have $|a + b| \leq \max(|a|, |b|) < 1$ and $|ca| = |c||a| < 1$. Moreover, it is a prime ideal since $|a| = |b| = 1$ yields $|ab| = 1$. Since $k[x]$ is a PID, $P = (p(x))$ for some prime polynomial. Now let $\gamma = |p(x)|$ so that $0 < \gamma < 1$. Let $f \in k(x)$ be arbitrary. We may write $f = p(x)^k \frac{a(x)}{b(x)}$ for some $k \in \mathbb{Z}$, $a(x), b(x) \in k[x]$ with $a(x), b(x) \notin (p(x))$. This yields $|a(x)| = |b(x)| = 1$, and consequently $|f| = |p(x)^k| = \gamma^k = \gamma^{v_p(f)}$. This is the valuation defined in Example 20.

Case II. $|x| > 1$: Let $b = b_0 + \cdots + b_m x^m$ be an arbitrary element of $k[x]$. Observe that for each $0 \leq i < m$, we have $|b_m x^m| = |x^m| = |x|^m > |x|^i = |b_i x^i|$. Hence Exercise 3 tells us $|b| = |x|^m$. Put $\gamma = |x|^{-1}$, so that $0 < \gamma < 1$. If $f \in k(x)$ is an arbitrary element, then we write $f = x^{-k} \frac{a(x)}{b(x)}$ for some $k \in \mathbb{Z}$, $a(x), b(x) \in k[x]$ with $(a(x), x) = 1 = (b(x), x)$. Hence $|a(x)| = |b(x)| = 1$ and therefore $|f| = |x^{-k}| = \gamma^k$. This is the valuation defined in Example 21.

□

5 THE RING OF p-ADIC INTEGERS

Recall that the ring $\mathbb{Z}_p$ of p-adic integers is defined by

$$\begin{aligned}\mathbb{Z}_p &= \varprojlim \mathbb{Z}/(p^k) \\ &= \{(x_0, x_1, x_2, \cdots) \in \prod \mathbb{Z}/(p^i) \mid x_n \equiv x_{n-1} \pmod{p^n}\}.\end{aligned}$$

An element of $\prod \mathbb{Z}$ can be veiwed as a sequence of integers. It has been defined by the inverse limit of $\mathbb{Z}/(p^n)$. The explicit ring structure of it is given as follows. For $\{x_n\}, \{y_n\} \in \mathbb{Z}_p$, it can be checked that $\{x_n + y_n\}$, $\{x_n y_n\}$ are elements of $\mathbb{Z}_p$. Moreover, there is a natural embedding $\mathbb{Z} \to \mathbb{Z}_p$ given by $a \mapsto \{a\} = (a, a, a, \cdots)$. Hence $(\mathbb{Z}_p, +, \cdot, \{0\}, \{1\})$ forms a commutative ring, the *ring of p-adic integers*.
The constraint $x_n \equiv x_{n-1} \pmod{p^n}$ emposes that such a sequence $\{x_n\}$ must form a Cauchy sequence with respect to the valuation $|\cdot|_p$ on $\mathbb{Q}$. Hence $\mathbb{Z}_p$ may be regarded as the completion of $\mathbb{Z}$ with respect to $|\cdot|_p$ We shall come back to this soon.
Any two elements $(x_0, x_1, \cdots)$ and $(y_0, y_1, \cdots)$ of $\mathbb{Z}_p$ are the same if and only if $x_i \equiv y_i \pmod{p^{i+1}}$. Hence, in particular, translation is an identity map on $\mathbb{Z}_p$, i.e., $(x_0, x_1, x_2, \cdots) = (0, x_0, x_1, \cdots)$.
Note that $\varprojlim$ is an exact functor.

Theorem 7. $(x_0, x_1, \cdots) \in (\mathbb{Z}_p)^\times \iff p \nmid x_0$

Proof. ($\Longrightarrow$) From $\{x_n\}\{y_n\} = \{1\}$, we have $x_n y_n \equiv 1 \pmod{p^{n+1}}$. In particular, $x_0 y_0 \equiv 1 \pmod{p}$. Thus $p \nmid x_0$.

($\Longleftarrow$) Assume $p \nmid x_0$. Since $x_i \equiv x_{i-1} \pmod{p^i}$, we have

$$x_n \equiv x_{n-1} \equiv \cdots \equiv x_0 \pmod{p}.$$

so that $p \nmid x_n$. Recall that $a \in \mathbb{Z}/(n)$ is unit iff $(a, n) = 1$. Consequently, for any n, we have $x_n \in (\mathbb{Z}/(p^{n+1}))^\times$ and hence we may find y_n such that

$$x_n y_n \equiv 1 \pmod{p^{n+1}}.$$

Now we show that the sequence $\{y_n\}$ is an element of $\mathbb{Z}_p$. Note that $x_n \equiv x_{n-1} \pmod{p^n}$ says x_n and x_{n-1} represent the same element of $(\mathbb{Z}/(p^n))^\times$, so that their inverse elements y_{n-1}, y_n also represent the same element of $(\mathbb{Z}/(p^n))^\times$. This shows $\{y_n\} \in \mathbb{Z}_p$.

□

From this theorem it follows that a rational integer a, considered as an element of $\mathbb{Z}_p$, is a unit if and only if $p \nmid a$. If this condition holds, then a^{-1} belongs to $\mathbb{Z}_p$. Hence any rational integer b is divisible by such an a in $\mathbb{Z}_p$, that is, any rational number of the form $\frac{b}{a}$, where a and b are integers and $p \nmid a$, belongs to $\mathbb{Z}_p$. Rational numbers of this ttype are called *p-integers*. They clearly form a ring, the locall ring $\mathbb{Z}_{(p)}$. We can now formulate the above result as follows:

Corollary 5. There is an embedding of the local ring $\mathbb{Z}_{(p)}$ into $\mathbb{Z}_p$ given by

$$\frac{b}{a} \longmapsto (b, b, \cdots)(a, a, \cdots)^{-1}$$

However, there is no embedding $\mathbb{Q} \to \mathbb{Z}_p$ since $\mathbb{Z}_p$ is a division ring whereas $\mathbb{Q}$ is not.

Example 25. $\{2\} \in (\mathbb{Z}_3)^\times$ since $3 \nmid 2$. $(2,2,2,\cdots)(y_0,y_1,\cdots) = (1,1,1,\cdots)$. By easy calculation, one has $(y_0,y_1,\cdots) = (2,5,14,41,\cdots) = (2, 2+1\cdot 3, 2+1\cdot 3+1\cdot 3^2, 2+1\cdot 3+1\cdot 3^2+1\cdot 3^3)$. Hence $y_n = 1+\sum_{i=0}^{n} 3^i$.

Consider $(k,|\cdot|)$, the field k absolute value. If $|r|<1$, then $\sum_{n=0}^{\infty} r^n = \frac{1}{1-r}$. In fact, the inverse is also true.

Definition 20. The field of p-adic numbers $\mathbb{Q}_p$ is defined by the field of quotient of the ring of p-adic integers $\mathbb{Z}_p$.

Theorem 8. (1) $0 \neq \alpha \in \mathbb{Z}_p \Longrightarrow \exists!\ k \in \mathbb{Z}^+$ and $\exists u \in (\mathbb{Z}_p)^\times$ such that $\alpha = p^k u$.

(2) $0 \neq \alpha \in \mathbb{Q}_p \Longrightarrow \exists!\ k \in \mathbb{Z}$ and $\exists u \in (\mathbb{Z}_p)^\times$ such that $\alpha = p^k u$.

Proof. (1) Proof by example. Recall that the translation $(x_0,x_1,x_2,\cdots) \mapsto (0,x_0,x_1,\cdots)$ is an identity map on $\mathbb{Z}/p$. Hence

$$\begin{aligned}(0,0,2p^2,2p^2+p^3,2p^2+1p^3+3p^4) &= (2p^2,2p^2+p^3,2p^2+p^3+3p^4)\\ &= p^2(2,2+p,2+p+3p^2,\cdots)\end{aligned}$$

(2) Let α be a nonzero element of $\mathbb{Q}_p$. Then $\alpha = a/b$ where $a,b \in \mathbb{Z}_p - \{0\}$. By part (1), one can write $a = p^s u$ and $b = p^t v$ for some $s,t \in \mathbb{Z}$ and $u,v \in (\mathbb{Z}_p)^\times$. Then $\alpha = p^{s-t}\frac{u}{v}$ and $\epsilon = u/v \in (\mathbb{Z}_p)^\times$.

□

Definition 21. Let $\alpha \in \mathbb{Q}_p$ as in Theorem 8-(2). The map $\alpha \longmapsto |\alpha|_p := \frac{1}{p^k}$ is called the *p-adic valuation* on $\mathbb{Q}_p$.

Exsercise : Show that the p-adic valuation on $\mathbb{Q}$ is well-defined.

Corollary 6. The p-adic integer α determined by the sequence $\{x_n\}$ is divisible by p^k if and only if $x_n \equiv 0 (\text{mod } p^{n+1})$ for all $n = 0,1,\cdots,k-1$. That is, $\alpha = (0,\cdots,0,x_k,x_{k+1},\cdots)$.

Corollary 7. The p-adic integer α is divisible by β if and only if $|\alpha|_p \leq |\beta|_p$.

HW 6. Let $x \in \mathbb{Z}_p$ and let $(a_0, a_0+a_1p, a_0+a_1p+a_2p^2,\cdots)$ be the canocial sequence that determines x. We define the *p-adic expansion* of x by $x = [a_0a_1a_2\cdots]_p$. Then show that x has *periodic* p-adic expansion if and only if $x = \phi(\frac{b}{a})$ for some $\frac{b}{a} \in \mathbb{Z}_{(p)}$.

Definition 22. The sequence $\{\zeta_n\} = (\zeta_0,\zeta_1,\zeta_2,\cdots)$ of p-adic numbers converges to a p-adic number ζ if

$$\lim_{n\to\infty} |\zeta_n - \zeta|_p = 0.$$

Theorem 9. If the p-adic integer α is determined by the sequence $\{x_n\}$ of rational integers, then this sequence converges to α. An arbitrary p-adic number ζ is a limit of a sequence of rational numbers.

Proof. Observe that

$$\begin{aligned}(x_0,x_1,\cdots)-(x_n,x_n,\cdots) &= (x_0-x_n,x_1-x_n,\cdots,x_{n-1}-x_n,0,x_{n+1}-x_n,\cdots)\\ &= (0,\cdots,0,x_{n+1}-x_n,x_{n+2}-x_n,\cdots)\end{aligned}$$

since $x_i - x_n \equiv (\text{mod } p^{i+1})$ for $i = 0,1,\cdots,n-1$. Thus we have the congruence

$$\alpha \equiv x_n (\text{mod } p^{n+2}) \quad \forall n \in \mathbb{N}$$

and therefore $|\alpha - (x_n,x_n,\cdots)|_p \leq 1/p^{n+1} \to 0$. This shows $x_n \to \alpha$. □

Proposition 11. Let $(k, |\cdot|)$ be a valuation. If it is complete, then

$$\sum_{n=0}^{\infty} a_n \text{ converges} \iff \lim_{n\to\infty} a_n = 0\,.$$

Proof. We want to show the partial sum forms a Cauchy sequence. Observe the difference of the partial sum S_n and S_{n+k} converges to zero since we have

$$|a_{n+k} + \cdots + a_n| \leq \max_{n\leq i\leq n+k}(|a_i|)$$

and the right hand side converges to zero as $n \to \infty$ by the hypothesis. □

Define Lie group on p-adic field.
Global field : $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Local field : $\mathbb{Q}_p, \overline{\mathbb{Q}_p}, \widehat{\mathbb{Q}_p}_{p[t]\text{-adic}}$
Completion. $k, |\cdot|$ has completion $\widehat{k}$. See J2, B-S.

HW 7. $\mathbb{Z}_p$: complete metric space. On the other hand, $\mathbb{Z}_p = \{(x_0, x_1, \cdots) \in \prod_{n=1}^{\infty} \mathbb{Z}/(p^n) \mid x_n \equiv x_{n-1} (\text{mod } p^n)\}$. Note that each $\mathbb{Z}/(p^n)$ is discrete topology, and their product is totally disconnected and compact. Are those two interpretation have the same topology?

Proof. The two topologies are equivalent. To begin the proof, recall that every element $x \in \mathbb{Z}_p$ is determined by a canonical sequence, i.e., $x = (x_0, x_1, x_2, \cdots)$ with $x_i \equiv x_{i+1} (\text{mod } p^{i+1})$ and $0 \leq x_i < p^{i+1}$. Hence every canonical sequence has the from

$$\{a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \cdots\}. \tag{$*$}$$

where $0 \leq a_i < p$.
First we show the product topology is finer than metric topology. Let $\alpha \in \mathbb{Z}_p$. We first show the open ball $B(\alpha, r) := \{x \in \mathbb{Z}_p \mid |x - \alpha| < r\}$ is open in the product topology. Let $y = (y_0, y_1, \cdots) \in B(\alpha, r)$. Then there is a natural number such that $B(y, \frac{1}{p^k}) \subset B(\alpha, r)$. Note that $|z - \alpha| < \frac{1}{p^k}$ if and only if the first k coordinates of z and α are the same, which follows immediately from the cannocial expression $(*)$. Hence we have

$$B(y, \frac{1}{p^k}) = \{a_0\} \times \cdots \times \{a_{k-1}\} \times \prod_{n=k}^{\infty} \mathbb{Z}/(p^n)$$

where the right hand side is an open set in the product topology. Thus the open ball $B(x, r)$ is open in the product topology.
On the other hand, let $U := U_0 \times \cdots \times U_r \times \prod_{n=r+1}^{\infty} \mathbb{Z}/(p^n)$ be an arbitrary open set in the product topology, where each U_i is a subset of the discrete space $\mathbb{Z}/(p^i)$ for $i = 0, 1, \cdots, r$. Let $x = (x_0, x_1, \cdots)$ be a point in U. Let $y = (y_0, y_1, \cdots) \in B(x, 1/p^{r+1})$. It follows that $x_i = y_i$ for $i = 0, 1, \cdots, r$ and hence $y \in U$; this shows $B(x, 1/p^{r+1}) \subset U$, and hence U is open in the metric topology. This shows the two "natural" topologies on $\mathbb{Z}_p$ are equivalent. □

6 Completion of a Field

$\mathbb{Q}_\infty \rightsquigarrow \mathbb{R}$, $\mathbb{Q}_p \rightsquigarrow \widehat{\mathbb{Q}}$.

Definition 23. Let k be a field with an absolute value $|\cdot|$. A sequence $\{a_n\}$ of elements of F is called a Cauchy sequence if given any real $\epsilon > 0$, there exists a positive integer $N = N(\epsilon)$ such that

$$|a_m - a_n| < \epsilon$$

for all $m, n \geq N$. F is said to be complete relative to $|\cdot|$ if every Cauchy sequence of elements of F converges($\lim a_n$ exists).

Let $\mathscr{C}$ be the set of all Cauchy sequence in k. If $\{a_n\}, \{b_n\} \in k$, we define $\{a_n\} + \{b_n\} = \{a_n + b_n\}$, $\{a_n\}\{b_n\} = \{a_n b_n\}$. These are contained in $\mathscr{C}$. If $a \in k$, we let $\{a\}$ be the constant sequence all of whose terms are a. Then $(\mathscr{C}, +, \cdot, \{0\}, \{1\})$ is a commutative ring contaning the subring of constant sequences that is isomorhic to k under $a \mapsto \{a\}$. (in fact, a k-algebra.)

Note 2. The completion in analysis is the quotient $\mathscr{C}/\sim$ where the equivalence relation $\sim$ is given by $\{a_n\} \sim \{b_n\}$ iff $\lim(a_n - b_n) = 0$.

Proposition 12. Let $\mathscr{C}$ be the set of all Cauchy sequence in $(k, |\cdot|)$. If $\{a_n\}, \{b_n\} \in k$, we define $\{a_n\} + \{b_n\} = \{a_n + b_n\}$, $\{a_n\}\{b_n\} = \{a_n b_n\}$. These are contained in $\mathscr{C}$. If $a \in k$, we let $\{a\}$ be the constant sequence all of whose terms are a. Then $(\mathscr{C}, +, \cdot, \{0\}, \{1\})$ is a commutative ring contaning the subring of constant sequences that is isomorhic to k under $a \mapsto \{a\}$. Now define $\mathscr{M} := \{\{a_n\} \in \mathscr{C} \mid \lim a_n = 0\}$. Then following statements are true.

(a) $\mathscr{M}$ is a maximal ideal in $\mathscr{C}$.

(b) By part (a), $\widehat{k} := \mathscr{C}/\mathscr{M}$ is a field. We may identify k as a subfield of $\widehat{k}$ with the natural embedding $a \mapsto \overline{\{a\}} = \{a\} + \mathscr{M}$. Then we may extend $|\cdot|$ on k to $\widehat{k}$ as follows:

$$\left|\overline{\{a_n\}}\right|' := \lim_{n\to\infty} |a_n|$$

(note that $||a_n| - |a_m|| \leq |a_n - a_m|$ shows $\{|a_n|\}$ is a Cauchy sequence of real numbers, so $\lim|a_n|$ exists in $\mathbb{R}$.) This defines a well-defined absolute value on $\widehat{k}$.

(d) k is dense in $\widehat{k}$ relative to the topology provided by the absolute value $|\cdot|'$.

(c) $(\widehat{k}, |\cdot|')$ is complete.

Proof. (a) Suppose for contrary that there is a proper ideal $\mathscr{M}'$ of $\mathscr{C}$ properly containing $\mathscr{M}$, and let $\{a_n\} \in \mathscr{M}' \setminus \mathscr{M}$. Then there is a nonzero element $\alpha \in k$ such that $\alpha = \lim_{n\to\infty} a_n$. Then there is a positive integer N such that whenever $n \geq N$, we get $a_n \neq 0$. Now define a sequence $\{b_n\}$ by $b_k := 1$ for $k \leq N$ and $b_k = a_k$ for $k \geq N$. Clearly $\{b_n\} \in \mathscr{C}$ and $\{c_n\} = \{a_n\} - \{b_n\} \in \mathscr{M}$.

I claim that the sequence $\{b_n^{-1}\}$ is a Cauchy sequence. Generally we will show that any Cauchy sequence $\{w_n\} \notin \mathscr{M}$ such that $w_n \neq 0$ for all n has its inverse sequence $\{w_n^{-1}\}$ which is also a Cauchy sequence. Note that $\{|w_n|\}$ forms a Cauchy sequence in $\mathbb{R}$ since $||w_n| - |w_m|| \leq |w_n - w_m|$ holds. Since $\mathbb{R}$ is complete, $|w_n|$ converges to a real number, say L, and $L \neq 0$ by the hypothesis $\{w_n\} \notin \mathscr{M}$. Now

$$|w_n - w_m| = |w_n(1 - w_m w_n^{-1})| = |w_n||1 - w_m w_n^{-1}| \to 0$$

and $|w_n| \to L \neq 0$ yields $|1 - w_m w_n^{-1}| \to 0$. Hence we obtain

$$|w_n^{-1} - w_m^{-1}| = |w_m^{-1}(w_m w_n^{-1} - 1)| = |w_m^{-1}||w_m w_n^{-1} - 1| \to \frac{1}{L} \cdot 0 = 0$$

and thereby showing that $\{w_n^{-1}\}$ forms a Cauchy sequence. This shows the claim.

Now observe that

$$1 = \{b_n\}\{b_n^{-1}\} = (\{a_n\} - \{c_n\})\{b_n^{-1}\} = \{a_n\}\{b_n^{-1}\} - \{c_n\}\{b_n^{-1}\} \in \mathscr{M}'$$

which contradicts the choice of $\mathscr{M}'$. Therefore $\mathscr{M}$ is a maximal ideal in $\mathscr{C}$.

(b) To show the value of $\left|\overline{\{a_n\}}\right|'$ does not depend on the choice of representative, let $\{a_n\}$, $\{b_n\}$ be two elements of $\mathscr{C}$ which represent the same element of $\widehat{k}$, i.e., $\{a_n\} - \{b_n\} = \{a_n - b_n\} \in \mathscr{M}$. Now

$$||a_n| - |b_n|| \leq |a_n - b_n| \to 0$$

yields $\lim_{n\to\infty} |a_n| = \lim_{n\to\infty} |b_n|$. Hence $|\cdot|'$ on $\widehat{k}$ is well-defined.

We now show $|\cdot|'$ defines an absolute value on $\widehat{k}$.

(i) $|\alpha|' > 0$ if $a \neq 0$ and $|0| = 0$

Let $\alpha = \{a_n\} + \mathscr{M} \in \widehat{k}$. $|\alpha|' \neq 0$ means $\lim_{n\to\infty} a_n \neq 0$ and hence $\lim_{n\to\infty} |a_n| \neq 0$. Since the limit of a sequence of nonnegative real numbers is always nonnegative, this yields $|\alpha|' > 0$. On the other hand, $\alpha = 0$ means $\alpha \in \mathscr{M}$ so that $a_n \to 0$; thus $|a_n| \to 0$ and hence $|\alpha|' = 0$.

(ii) $|\alpha\beta|' = |\alpha|'|\beta|'$

Let $\alpha = \overline{\{a_n\}}$, $\beta = \overline{\{b_n\}} \in \mathscr{C}$. Then we have

$$|\alpha\beta|' = \lim_{n\to\infty} |a_n b_n| = \lim_{n\to\infty} |a_b||b_n| = \lim_{n\to\infty} |a_n| \lim_{n\to\infty} |b_n| = |\alpha|'|\beta|'.$$

(iii)' $|\alpha + \beta|' \leq |\alpha|' + |\beta|'$

Let $\alpha = \overline{\{a_n\}}$, $\beta = \overline{\{b_n\}} \in \mathscr{C}$. Then we have

$$|\alpha + \beta|' = \lim_{n\to\infty} |a_n + b_n| \leq \lim_{n\to\infty} |a_b| + |b_n| = \lim_{n\to\infty} |a_n| + \lim_{n\to\infty} |b_n| = |\alpha|' + |\beta|'.$$

(c) It suffices to show that any element $\overline{\alpha} \in \widehat{k}$ is the limit of a sequence of elements in k. Indeed, if $\overline{\alpha} = \{a_n\} + \mathscr{M}$, then $\lim_{n\to\infty} a_n = \overline{\alpha}$. Hence k is dense in $\widehat{k}$ relative to the metric topology induced by $|\cdot|'$.

(d) We need to show that every Cauchy sequence $\{\alpha_n\}$ in $\widehat{k}$ converges to some element α in $\widehat{k}$. Now let $\{\alpha_n\}$ be an arbitrary Cauchy sequence in $\widehat{k}$. Since k is dense in $\widehat{k}$ relative to the metric topology given by $|\cdot|'$, for each α_n we can choose an element $a_n \in k$ such that $|\alpha_n - a_n|' < 1/n$. Then $\{a_n\}$ forms a Cauchy sequece in k, since

$$|a_n - a_m|' \leq |a_n - \alpha_n|' + |\alpha_n - \alpha_m|' + |\alpha_m - a_m|'$$

where the right hand side can be as small as we please by taking large N such that $n, m > N$, noting that $\{\alpha_n\}$ is a Cauchy sequence. Then $\{a_n\}$ converges to $\overline{a} := \overline{\{a_n\}} = \{a_n\} + \mathscr{M}$ in $\widehat{k}$. But then $\{\alpha_n\}$ also converges to $\overline{a}$, since

$$|\alpha_n - \overline{a}|' \leq |\alpha_n - a_n| + |a_n - \overline{n}|$$

and the right hand side approches to zero as $n \to \infty$. This shows $(\widehat{k}, |\cdot|')$ is a complete metric space.

□

So far we have seen that any field k with absolute value $|\cdot|$ has a completion k with an absolute value $|\cdot|'$ in the sense that

(1) $\widehat{k}$ is an extension field of k and has an absolute value that is an extension of the given absolute value

(2) $\widehat{k}$ is complete relative to the absolute value $|\cdot|'$

(3) k is dense in $\widehat{k}$ relative to the topology provided by the absolute value.

We now establish the uniqueness of such completion. More generally we consider two fields $\widehat{k_i}$ for $i = 1,2$, which are complete relative to absolute value $||_i$ and let k_i be a dense subfield of $\widehat{k_i}$. Suppose we have an isomorphism $s : k_1 \to k_2$ that is *isometric* in the sense that $|a_1| = |sa_2|$ for $a \in \mathbb{F}_1$. Then s is a continuous map of k_1 into $\widehat{k_2}$ and since k_1 is dense in $\widehat{k_1}$, s has a unique extension to a continuous map $\overline{s} : \widehat{k_1} \to \widehat{k_2}$. This is easily seen to be a homomorphism, and since $\overline{s^{-1}}$ is a homomorphism and $s^{-1}s = 1_{k_1}$ and $ss^{-1} = 1_{k_2}$ imply $\overline{s^{-1}}\,\overline{s} = 1_{\widehat{k_1}}$, $\overline{s}\,\overline{s^{-1}} = 1_{\widehat{k_2}}$, it follows that $\overline{s}$ is an isomorphism. It is clear also that $\overline{s}$ is unique and is isometric. Hence we obtain

Theorem 10. If $\widehat{k_i}$, $i = 1,2$, is complete relative to an absolute value and k_i is a dense subfield of $\widehat{k_i}$, then any isometric isomorphism $s : k_1 \to k_w$ has a unique extension to an isometric isomorphsm $\overline{s} : \widehat{k_1} \to \widehat{k_2}$. This can be summarized by the following commutative diagram

$$\begin{array}{ccc} \widehat{k_1} & \overset{\exists!\overline{s}}{\dashrightarrow} & \widehat{k_2} \\ \uparrow & \text{isometric iso.} & \uparrow \\ k_1 & \xrightarrow[\text{isometric iso.}]{s} & k_2 \end{array}$$

Corollary 8. Let k be a field with absolute value $|\cdot|$. Let $\widehat{k}$ be a completion satisfying the three conditions (1),(2), and (3) above. Such completion is unique up to an isometric isomorphism.

Proof. Put $k_1 = k_2 = k$ in Theorem 10. □

If we complete $\mathbb{Q}$ relative to its usual absolute value $|\cdot|_\infty$ we obtain classically the field $\mathbb{R}$ of real numbers. On the other hand,

Theorem 11. The completion of $(\mathbb{Q}, |\cdot|_p)$ is algebraically homeomorphic to the $\mathbb{Q}_p$.

Proof. We first consider the closure $\overline{\mathbb{Z}}$ of $\mathbb{Z}$ in the completion $\widehat{Z}$ relative to $||_p$. An element $\alpha \in \overline{\mathbb{Z}}$ is the limit in $\widehat{\mathbb{Q}}$ of a sequence of integers a_i. Thus if $\alpha, \beta \in \overline{Z}$, then there are converging sequences $a_n \to \alpha$ and $b_n \to \beta$, so that $\alpha + \beta = \lim(a_n + b_n)$ and $\alpha\beta = \lim a_n b_n$ shows $\overline{Z}$ is a subring of $\widehat{\overline{Q}}$.
Then we define a ring homomorphism $\phi : \overline{\mathbb{Z}} \to \mathbb{Z}_p$. For $\alpha \in \overline{\mathbb{Z}}$, $\exists\, x_i \in \mathbb{Z}$ such that $|\alpha - x_i| < \frac{1}{p^{i+2}}$. Since we have

$$|x_{i+1} - x_i|_p \le |x_{i+1} - \alpha| + |\alpha - x_i| \le \frac{1}{p^{i+1}} + \frac{1}{p^{i+2}} \le \frac{1}{p^{i+1}},$$

the map the following map

$$\phi : \overline{\mathbb{Z}} \to \mathbb{Z}_p, \quad \alpha \mapsto (x_0, x_1, x_2, \cdots)$$

is well-defined and clearly a ring homomorphism. It is straightforward to check that this map is actually a ring isomorphism. Hence we may identify $\overline{\mathbb{Z}}$ with $\mathbb{Z}_p$.
Now let $V_{\mathbb{Q}} := \{|a|_p \mid a \in \mathbb{Q}\}$ be the value group. Observe that this is a discrete subset of $\mathbb{R}$, hence closed. Thus we have $V_{\mathbb{Q}} = \{|\alpha| \mid \alpha \in \widehat{\mathbb{Q}}\}$. Hence given any $\beta \neq 0$ in $\widehat{\mathbb{Q}}$ there exists an $e \in \mathbb{Z}$ such that $|\beta| = |p^e|$, so $\alpha = \beta p^{-e}$ satisfies $|\alpha| = 1$. Then we may write $\alpha = \lim a_i$ where $a_i = \frac{b_i}{c_i}$ and $(b_i, p) = 1 = (c_i, p)$. Now there exists $x_i \in \mathbb{Z}$ such that $x_i c_i \equiv b_i (\mathrm{mod}\ p^i)$. Then $|x_i - \frac{b_i}{c_i}| = \frac{1}{p^i}$ and so $\alpha = \lim x_i \in \overline{\mathbb{Z}} = \mathbb{Z}_p$. It follows that every element of $\widehat{Q}$ has the form αp^e for $\alpha \in \mathbb{Z}_p$. Thus $\widehat{\mathbb{Q}}$ is contained in the field of fraction $\mathbb{Q}_p$ of $\mathbb{Z}_p$; by the minimality of the field of fraction, we see that $\widehat{\mathbb{Q}} = \mathbb{Q}_p$. □

Ring structure of $\mathbb{Z}_p$. Let $\alpha \in \mathbb{Z}_p$ be a nonzero element. Then we can write $\alpha = p^k \epsilon$ for some $k \geq 0$ and $\epsilon \in (\mathbb{Z}_p)^\times$.

HW 8. (1) Show that $\mathbb{Z}_p$ is a Euclidean domain.

(2) Show that p is the only irreducible element in $\mathbb{Z}_p$. Hence every ideal is of the form $p^k \mathbb{Z}_p$ for some $k \geq 0$.

(3) Show that $\mathbb{Z}/p^k\mathbb{Z} \approx \mathbb{Z}_p/p^k\mathbb{Z}_p$. (see the localization exercise. Also B-S, p25 Corollary)

$\mathbb{Z}_p$ is a typical example of "discrete valuation ring(DVR)". "Discrete" means that the value group except 0 is a cyclic group generated by p. DVR is an example of Dedekind domain. $p^k\mathbb{Z}_p = (p\mathbb{Z})^k$.
A finite field extension K of $\mathbb{Q}$ is called *a number field*. Extend $|\cdot|_p$ to K. How many different ways?

Theorem 12 (Hasse-Minkovski)**.** Let $f(x_1, \cdots, x_n)$ be a quadratic form with rational coefficients. Then

$$\exists a_1, \cdots, a_n \in \mathbb{Q} \text{ such that } f(a_1, \cdots, a_n) = 0 \iff \exists b_1, \cdots, b_n \in \mathbb{Q}_p \text{ such that } f(b_1, \cdots, b_n) = 0 \text{ for all } p.$$

This theorem is a prime example of the Local-Global princible, i.e., globally true iff locally true everywhere.

Proof. B-S. □

7 INTRODUCTION TO ALGEBRAIC GEOMETRY

References : Fulton, Algebraic Curves. (classical language). Hartshorn(Modern Language, Scheme language), EGA, SGA, $4\frac{1}{2}$: Etale cohomology
Let k be an algebraically closed field. Let $\mathbb{A}^n_k := k^n$ be the *affine n-space*. Define Zariski topology on $\mathbb{A}^n_k$ by defining the closed sets as the zero set of polynomials. In other words, the only continuous function $k^n \to k$ relative to this topology is the polynomial functions.
"Mathematicians dream"
Lie groups over local fields : $\mathrm{Sp}_{2n}(\overline{\mathbb{Q}_p})$, one more
In analytic geometry, we consider the functions $\mathbb{C}^n \to \mathbb{C}$ analytic functions.
GAGA(geometric algebra=geometric analysis) principle

Notation. k : algebraically closed field. $k^n = \mathbb{A}^n$: affine n-space. Put $A = k[x_1, \cdots, x_n]$.

Zariski topology on $\mathbb{A}^n$.
Let S be a subset of A. Then the closed sets are given by the zero set of sets of polynomials S, i.e., $Z(S) = \{a \in k^n \mid f(a) = 0 \, \forall f \in S\})$ where $S \subset A$. Note that $Z(S) = Z(\langle S \rangle)$. To see this defines a topology, we need to check if artitrary intersection and finite union of closed sets are closed. The empty set and whole space is closed since $Z(1) = \emptyset$, $Z(0) = \mathbb{A}^n$.

Example 26. $k = \mathbb{A}^1$.

(1) for $f \in k[x]$ we have $|Z(f)| < \infty$.

(2) for nonempty $S \subset k[x]$, we have $Z(S) = \bigcap_{f \in S} Z(f)$ and has finite cardinality.

Hence closed sets of $\mathbb{A}^1$ are finite sets.

Define a map sending a subset of $\mathbb{A}^n$ to a subset of A, by

$$I(Y) = \langle f \in A \mid f(y) = 0 \, \forall y \in Y \rangle \text{ideal of} A.$$

Obserce that

(1) $S_1 \subset S_2 \Rightarrow I(S_1) \supset I(S_2)$

(2)

By Hilbert basis theorem($A = k[x_1, \cdots, x_n]$ is Noetherian), $Z(S) = Z(\langle S \rangle) = Z(f_1, \cdots, f_r)$ for some polynomials $f_1, \cdots, f_r \in S$. Hence the closed sets in Zariski topology is the zero sets of finite number of polynomials.

HW 9. Let X be a subset of $\mathbb{A}^n$.

(1) $X \subset Z(I(X))$

(2) $Z(I(X)) = \overline{X}$ (topological closure)

(3) $ZIZ(\mathfrak{a}) = Z(\mathfrak{a})$

(4) Let $\mathfrak{a}$ be an ideal of A. The *radical* $\sqrt{\mathfrak{a}}$ is the ideal defined by

$$\sqrt{\mathfrak{a}} := \{f \in A \mid f^r \in \mathfrak{a} \text{ for some } r \geq 1\}.$$

Then it holds that $IZ(\mathfrak{a}) = \sqrt{\mathfrak{a}}$. (Hillbert's Nullstellensatz)

(5) An ideal $\mathfrak{a}$ of A is a *radical ideal* if $\sqrt{\mathfrak{a}} = \mathfrak{a}$. Then $\sqrt{I(S)}$ is a radial ideal.

(6) $IZI(X) = I(X)$

Note that (4) in the above homework is a weak form of Hilbert Nullstellensats. Its strong form is that for every proper ideal $\mathfrak{a}$ of A, we have $Z(\mathfrak{a}) \neq \emptyset$.

Example 27. $x^2 \in k[x]$. $\langle x^2 \rangle$ is not radical since $x \in \sqrt{\langle x^2 \rangle}$ and $Z(x) = Z(x^2) = \{0\}$.

HW 10. Show that a maximal ideal is a radical ideal.

Definition 24. Let X be a topological space. X is *reducible* if $X = X_1 \cup X_2$ for some non-empty closed sets X_1, X_2.

Note that every irreducible set is connected.

Example 28. $f(x,y) = xy$. $Z(f) = \{(x,y) \in \mathbb{A}^2 \mid xy = 0\} = Z(x) \cup Z(y)$. Note that $Z(x) = \{(x,y) \in \mathbb{A}^2 \mid x = 0\}$ is irreducible.

Hartshorn(or perhaps Fulton) : everything is irreducible.
Algebraic group is not necessarily irreducible.

Theorem 13 (Hilbert's Nullstellensatz)**.** Let k be an algebraically closed field and let $A = k[x_1, \cdots, x_n]$. Then the following hold:

(1) Every maximal ideal $m \subset A$ is of the form

$$m = (x_1 - a_1, \cdots, x_n - a_n) = I(P)$$

for some point $P = (a_1, \cdots, a_n) \in \mathbb{A}^n_k$.

(2) If $J \subsetneq A$ is a proper ideal, then $V(J) \neq \emptyset$.

(3) For every ideal $J \subset A$ we have

$$I(Z(J)) = \sqrt{J}$$

Proof. See Hulek, Elementary Algebraic Geometry. □

Corollary 9. For $A = k[x_1, \cdots, x_n]$, the maps V and I

$$\{\text{ideals of } A\} \overset{Z,I}{\longleftrightarrow} \{\text{subsets of } \mathbb{A}^n_k\}$$

induce the following bijections:

$$\begin{array}{ccc}
\{\text{radical ideals of } A\} & \overset{1:1}{\longleftrightarrow} & \{\text{subvarieties of } \mathbb{A}^n_k\} \\
\cup & & \cup \\
\{\text{prime ideals of } A\} & \overset{1:1}{\longleftrightarrow} & \{\text{irreducible subvarieties of } \mathbb{A}^n_k\} \\
\cup & & \cup \\
\{\text{maximal ideals of } A\} & \overset{1:1}{\longleftrightarrow} & \{\text{points of } \mathbb{A}^n_k\}
\end{array}$$

Proof. See HW 13. □

Definition 25 (Temporary)**.** Category of algebraic sets. Objects are the closed subsets of affine space. Morphism $\phi : X \subset \mathbb{A}^n \to Y \subset \mathbb{A}^m$ is a polynomial map, namely,

$$\phi(x_1, \cdots, x_1) = (f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n))$$

where each f_i is a polynoimal function.

But this definition has some problem. For instance, $\langle xy = 1 \rangle \subset \mathbb{A}^n$ is not an algebraic set according to this definition. More generally, the general linear group would not be an algebraic set. Hence it might be better to allow "rational functions" as being morphisms.

Definition 26 (Hartshorne)**.** Let k be a fixed algebraically closed field. A *variety over k*(or simply variety) is any affine, quasi-affine, projective, or quasi-projective variety as defined above. If X, Y are two varieties, a *morphism* $\phi : X \to Y$ is a continuous map such that for every open set $V \subset Y$, and for every regular function $f : V \to k$, the composition $f \circ \phi : \phi^{-1}(V) \to k$ is regular, i.e., ϕ carries regular functions to regular functions.

Clearly the composition of two morphisms is a morphism, so we have a category.

Definition 27. Let $A = k[x_1, \cdots, x_n]$ and X be an algebraic set. Then the *affine coordinate k-algebra of X* is defined by $k[X] := A/I(X)$. Note that this equals the k-algebra of polynomial functions on X.

Definition 28. An algebra A is *reduced* if it has no nonzero nilpotent, i.e., $a^r = 0$ for some $a \in A$ and $r \in \mathbb{N}$, then $a = 0$.

Note that $k[X]$ is a finitely generated reduced k-algebra. Next proposition implies that two algebraic sets X, Y are isomorphic if and only if their coordinate k-algebras $k[X]$, $k[Y]$ are isomorphic as k-algebra. It is also the first example of non-trivial categorical equivalence.
In the following propoisition, we regard the only the polynomial maps between two algebraic sets as morphisms.

Proposition 13. The category of algebraic set $\mathscr{AS}$ is *anit-equivalent* to the category of finitely generated reduced k-Algebra $\mathscr{A}$, by the full and faithful contravariant functor

$$\begin{array}{rcl} F : \mathscr{AS} & \longrightarrow & \mathscr{A} \\ X & \longmapsto & k[X] \\ \mathrm{Mor}(X, Y) & \xrightarrow{1:1} & \mathrm{Hom}_{k-Alg}(k[Y], k[X]) \\ f & \longmapsto & f^*. \end{array}$$

Proof. We first show that the map F defined above defines a full and faithful contravariant functor.

(i) F is a well-defined contravariant functor into $\mathscr{A}$. That F maps into $\mathscr{A}$ is clear; $k[X] = k[x_1, \cdots, x_n]/I(X)$ is finitely generated since $k[x_1, \cdots, x_n]$ is so(Hilbert's theorem). It is reduced if and only if $I(X)$ is radical, and it is the case here. Clearly the dual map f^* is a k-algebra homomorphism and is a contravariant functor.

(ii) Conversely, suppose we have a homomorphism $h : k[Y] \to k[X]$ of k-algebra. By definition $k[Y] = k[x_1, \cdots, x_n]/I(Y)$. Denote by $\overline{x_i}$ the image of x_i in $k[Y]$, and recall that $k[Y]$ is generated by the coordinate functions $\overline{y_1}, \cdots, \overline{y_m}$. Now suppose we have a map $\psi : X \to Y$ such that $\psi^* = h$. This means for the generators we have

$$\overline{y_i} \circ \psi = h(\overline{y_i}).$$

Hence we define $\psi : X \to \mathbb{A}^m \supset Y$ by $\psi(P) = (\zeta_1(P), \cdots, \zeta_n(P))$ where $\zeta_i := h(\overline{y_i})$. ψ is a polynomial map since each $h(\overline{y_i})$ is a polynomial functions on X.

We show next that the image of ψ is contained in Y. Since $Y = Z(I(Y))$, it suffices to show for any $P \in X$ and any $f = f(y_1, \cdots, y_m) \in I(Y)$ that $f(\psi(P)) = 0$. But

$$f(\psi(P)) = f(\zeta_1(P), \cdots, \zeta_n(P)).$$

Now f is a polynomial, and h is a k-algebra homomorphism, so we have

$$f(\zeta_1(P), \cdots, \zeta_n(P)) = h(f(\overline{y_1}, \cdots, \overline{y_n}))(P) = h(\overline{f(y_1, \cdots, y_m)})(P) = 0$$

since $f \in I(Y)$ so that $\overline{f} = 0$. So ψ defines a map from X to Y, which induces the given homomorphism h. In addition, such ψ uniquely exists according to the argument. This uniqueness yields that F is full and faithful.

(iii) In order to construct an inverse functor G we proceed as follows. For a finitely generated reduced k-algebra A choose generators $a_1, \cdots, a_n$ of A and consider the homomorphism

$$\pi : k[x_1, \cdots, x_n] \to A = k[a_1, \cdots, a_n],$$

given by $\pi(x_i) = a_i$. Hence we write $A \simeq k[x_1, \cdots, x_n]/J$ where $J = \ker \pi$ is a radical ideal. Now we set $G(A) = V(J)$. On the other hand, for any homomorphism $\phi : A \to B$, there is a unique polynomial map $h : G(B) \to G(A)$ according to part (ii), and we define $G(\phi) = h$. This shows G is a contravariant functor. Finally, observe that $k[V] = k[x_1, \cdots, x_n]/I(V(J)) = k[x_1, \cdots, x_n]/J \simeq A$, which shows $F \circ G \simeq id_{\mathscr{A}}$. On the other hand, we clearly have $G \circ F = id_{\mathscr{A}\mathscr{S}}$. This

□

So we only need to study the category of k-algebra for that of algebraic sets.

Lemma 1. Let X be any variety, and let $Y \subset \mathbb{A}^n$ be an affine variety. A map of sets $\psi : X \to Y$ is a morphism if and only if $x_i \circ \psi$ is a regular function on X for each i, where $x_1, \cdots, x_n$ are the coordinate functions on $\mathbb{A}^n$.

Proof. If ψ is a morphism, then the composition $x_i \circ \psi$ must be regular functions, by definition of a morphism. Conversely, suppose the $x_i \circ \psi$ are regular. Then for any polynomial $f = f(x_1, \cdots, x_n)$, $f \circ \psi$ is also regular on X and in particular, continuous. Now we show that ψ is continuous on X by showing that the inverse image of closed sets in Y under ψ is closed. Let $V = Z(J)$ be a closed set in Y. Since $k[x_1, \cdots, x_n]$ is Noetherian, J is finitely generated; write $J = \langle f_1, \cdots, f_r \rangle$ for some polynomials f_i. Then $V = \bigcap_{i=1}^r Z(f_i)$. Sinc $\psi^{-1}(V) = \bigcap_{i=1}^r \psi^{-1}(Z(f_i))$, and intersection of closed sets is closed, it suffices to show that $\psi^{-1}(Z(f_i))$ is closed in X. But since

$$\psi^{-1}(Z(f_i)) = (f_i \circ \psi)^{-1}(\{0\}),$$

which is the inverse image of the closed set $\{0\}$ under the continuous map $f_i \circ \psi$, we see $\psi^{-1}(Z(f_i))$ is closed in X. This shows $\psi : X \to Y$ is continuous.
Now we show ψ is a morphism, i.e., for any regular function g on any open subset $U \subset Y$, $g \circ \psi$ is regular on $\psi^{-1}(U)$. We need to show for any $P \in \psi^{-1}(U)$ that this function is locally rational. Since g is regular on U, it is regular on $\psi(P)$, hence there are polynomial functions $f, h \in k[x_1, \cdots, x_n]$ such that $g = f/h$ and h is nowhere vanishing on some open neighborhood $V_{\psi P} \subset U$ of ψP. Recall that we know the composite $f \circ \psi$ and $h \circ \psi$ are regular; hence those functions can be expressed as a fational functions near P. Let us write $f \circ \psi = p_1/q_1$ and $g \circ \psi = p_2/q_2$ which is valid on a small neighborhood $W \subset X$ of P. We may assume that W is small enough so that $\psi(W) \subset V_{\psi(P)}$.(e.g, take the intersection $W \cap \psi^{-1}(V_{\psi(P)})$.) Since h does not vanish near ψP(on $V_{\psi P}$), p_2 is never zero on $W \subset \psi^{-1}(V_{\psi(P)})$. Thus $g \circ \psi = \frac{f \circ \psi}{h \circ \psi} = \frac{p_1}{q_1} / \frac{p_2}{q_1} = \frac{p_1 q_2}{p_2 q_1}$ and $p_2 q_1$ does not vanish on W. This shows $f \circ \psi$ is regular on P. Since P was arbitrary, $g \circ \psi$ is regular on $\psi^{-1}(U)$. Therefore ψ is a morphism. This shows the Lemma. □

From now on we may assume every objects are commutative.

Definition 29. A topological space X is *Noetherian* if DCC(descending chain condition) holds for closed sets.

HW 11 (Hartshorne Ex 1.7)**.** Show the followings.

(a) Show that the following conditions are equivalent for a topological space X : (i) X is Noetherian; (ii) every nonempty family of closed subsets has a minimal element; (iii) X satisfies the ascending chain condition for open subsets; (iv) every nonempty family of open subsets has a maximal element

(b) A Noetherian topological space is *quasi-compact*, i.e., every open cover has a finite subcover.

(c) Any subset of a Noetherian topological space is Noetherian in its induced topology.

(d) A Noetherian space which is also Hausdorff must be a finite set with the discrete topology.

Proof. (a)

(i)⇔(ii) Let $\mathscr{F}$ be any family of closed sets. If there is no minimal element, then for any element $C \in \mathbb{F}$ we can find a smaller one $C' \subsetneq C'$ in F. Repeating this process , we get a strictly descending chain of infinite length $C \supsetneq C' \supsetneq \cdots$, which contradicts that X is Noetherian. Hence $\mathscr{F}$ has a minimal element.

Conversely, suppose every family of closed sets has a minimal element. Now given a descending chain of closed sets $C_1 \supset C_2 \supset C_3 \supset \cdots$, the collection $\mathscr{F} = \{C_i \mid i \in \mathbb{N}\}$ must have a minimal element, say C_n. Then for any $m \geq n$, we must have $C_m = C_n$ since $C_n \supset C_m$ and C_n is a minimal element. This shows X is Noetherian.

(i)⇔(iii) (iii) is the compliment of (i) and vice versa.

(ii)⇔(iv) (iv) is the compliment of (ii) and vice versa.

(b) Let X be a Noetherian space and $\bigcup_{\alpha \in I} X_\alpha$ be an open covering. We may suppose for contrary that there is no finite subcovering of this.(hence we assume $|I| = \infty$) We may further assume that this open covering is not redundant, i.e., $\bigcup_{\alpha \in I \setminus \{\beta\}} X_\alpha \subsetneq X$ for every $\beta \in I$. Now put $V_1 = X - X_1$, $V_2 = X - X_1 - X_2$, $V_3 = X - X_1 - X_2 - X_3$ and so on. Then we have a descending chain of closed sets

$$V_1 \supset V_2 \supset V_3 \supset \cdots.$$

By DCC, there is some n such that $V_n = V_m$ for all $m \geq n$. In particular, we have $V_{n+1} = V_n$, but this means $V_{n+1} = V_n - X_{n+1} = V_n$ and hence $X_{n+1} \subset \bigcup_{i=1}^{n} X_i$, contradicting the assumption. Thus X is quasi-compact.

(c) Let $Y \subset X$ be a subspace, and $V_1 \supset V_2 \supset \cdots$ be a descending chain of closed sets in Y. Let $\overline{V_i}$ be the closure of V_i in X. Since taking closure preserves inclusion, we get a descending chain of closeds sets in X:

$$\overline{V_1} \supseteq \overline{V_2} \supseteq \overline{V_3} \supseteq \cdots.$$

Since X is Noetherian, there is some $n \in \mathbb{N}$ such that $\overline{V_m} = \overline{V_n}$ whenever $m \geq n$. Note that for any closed subset $C \subset Y$ we have $C = Y \cap \overline{C}$; for, if we write $C = Y \cap V$ for some closed subset $V \subset X$, then $C \subset \overline{C} \subset V$, so that $C \subset Y \cap \overline{C} \subset Y \cap V = C$. Thus we have

$$V_m = Y \cap \overline{V_m} = Y \cap \overline{V_n} = V_n$$

and hence Y is Noetherian.

(d) Let X be Noetherian Hausdorrf space and suppose for contradiction that X is infinite. Pick two distinct points x, y and choose open separation U_1, V_1 of them; $x \in U_1$, $y \in V_1$, $U_1 \cap V_1 = \emptyset$. Either of $X \setminus U_1$ or $X \setminus V_1$ is infinite. We may assume the former. Then $X \setminus U_1$ is a subspace of X, which is again Noetherian(by (c)) and Hausdorff. In similar way, we can choose a nonempty open subset U_2 of $X \setminus U_1$ such that $X \setminus (U_1 \cap U_2)$ is infinite. Inductively, we choose open subset U_k of $X \setminus (U_1 \cup \cdots \cup U_{k-1})$ such that $X \setminus (U_1 \cup \cdots \cup U_k)$ is infinite. Now for each U_k, there is an open subset U_k' of X such that $U_k = U_k' \cap X \setminus (U_1 \cup \cdots \cup U_{k-1})$. Put $D_k = U_1' \cup \cdots \cup U_k'$. Then $D_1 \subset D_2 \subset \cdots$ is an ascending chain of open subsets of X and it never stabilizes for its construction. This contradicts the condition (iii) of part (a), and hence X must be finite. Since X is Hausdorff, every point set is closed and hence X has discrete topology.

□

Proposition 14. The affine n-space $\mathbb{A}^n$ is Noetherian space.

Proof. Recall that the polynomial ring $A := k[x_1, \cdots, x_n]$ is Noetherian. Hence ACC for ideals holds. This yields DCC for closed sets of $\mathbb{A}^n$. To see this, let

$$X_1 \supset X_2 \supset X_3 \cdots \tag{1}$$

be a descending chain of closed sets in $\mathbb{A}^n$. By the corollary of Hilbert's Nullstellensatz, every closed set in $\mathbb{A}^n$ is the zero set of some radical ideal. Hence we may write $X_i = Z(J_i)$ for some radical ideal $J_i \subset A$. Hence $(*)$ becomes

$$Z(J_1) \supset Z(J_2) \supset Z(J_3) \cdots$$

and hence we obtain an ascending chain of ideals

$$I(Z(J_1)) \subset I(Z(J_2)) \subset I(Z(J_3)) \cdots \tag{2}$$

By ACC for the Noetherian ring A, there is a natural number n such that $IZ(J_n) = IZ(J_m)$ for all $m \geq n$. But by Hilbert's Nullstellensatz (2), $(**)$ beceoms

$$J_1 \subset J_2 \subset J_3 \subset \cdots \subset J_n = J_{n+1} = J_{n+2} = \cdots. \tag{3}$$

Applying Z to (3), we get minimal element for the descending chain (1). Thus $\mathbb{A}^n$ is Noetherian. □

Remark 2. X is Noetherian and Hausdorff $\Longrightarrow |X| < \infty$
X is irreducible and Hausdorff $\Longrightarrow |X| = 1$
So we are interested in non-Hausdorff spaces.

HW 12. Let $X \subset \mathbb{A}^n_k$ be an affine algebraic set. Show that these followings are equivalent:

(i) X is irreducible.

(ii) every two nonempty open set in X have a nonempty intersection.

(iii) every nonempty open set in X is dense in X.

Proof. (i)$\Longleftrightarrow$ (ii) For any subsets U, V of X we have

$$U \cap V = \emptyset \quad \Longleftrightarrow \quad (X-U) \cup (X-V) = X. \tag{$*$}$$

Suppose X is irreducibe. Note that if both U, V are nonempty open and $U \cap V = \emptyset$, then X is a union of two nonempty closed subsets $X-U$ and $X-V$ which are properly contained in X. Since a closed subset of X is an intersection of X and a closed set of $\mathbb{A}^n_k$, and since X is closed, we see that closed subsets of X is closed in $\mathbb{A}^n_k$. Hence this contradicts that X is irreducible.

On the other hand, assume (ii). If X is not irreducible, then there are nonempty closed sets $C_1, C_2 \subset \mathbb{A}^n_k$ such that $C_1, C_2 \subsetneq X$ and $X = C_1 \cup C_2$. Put $U = X \cap C_1^C$ and $V = X \cap C_2^C$. They are nonempty open subsets of X, and but $(*)$ yields $U \cap V = \emptyset$. This contradictions shows X is irreducible.

(ii)$\Longleftrightarrow$ (iii) It follows from the fact that a subset $D \subset X$ is dense in X if and only if $D \cap U \neq$ for all open subset U of X.

□

Proposition 15. Let X be a closed subset in a Noetherian space. Then there are irreducible subsets $X_1, \cdots, X_r$ such that

$$X = X_1 \cup \cdots \cup X_r.$$

Such expression is unique if $X_i \nsubseteq X_j$ for all $i \neq j$. Such X_is are called *irreducible components of* X.

Standard agrument. Let $\mathfrak{C}$ be the collection of closed sets in X that violates the assertion. Since X is Noetherian, there is a minimal element $X \subset \mathfrak{C}$. We may assume X is not irreducible. Hence we can write $X = Y_1 \cup Y_2$ for some closed sets Y_1, Y_2. By the minimality, each Y_i is the union of some irreducible sets, so that X is a union of some irreducible sets, which is a contradiction. □

HW 13. Show that for $A = k[x_1, \cdots, x_n]$, the maps Z and I

$$\{\text{ideals of } A\} \overset{Z,I}{\longleftrightarrow} \{\text{subsets of } \mathbb{A}^n_k\}$$

induce the following bijections:

$$\begin{array}{ccc}
\{\text{radical ideals of } A\} & \overset{1:1}{\longleftrightarrow} & \{\text{subvarieties of } \mathbb{A}^n_k\} \\
\cup & & \cup \\
\{\text{prime ideals of } A\} & \overset{1:1}{\longleftrightarrow} & \{\text{irreducible subvarieties of } \mathbb{A}^n_k\} \\
\cup & & \cup \\
\{\text{maximal ideals of } A\} & \overset{1:1}{\longleftrightarrow} & \{\text{points of } \mathbb{A}^n_k\}
\end{array}$$

Proof. We know $Z(I(X)) = X$ and $I(Z(\mathfrak{a})) = \mathfrak{a}$ for every closed set $X \subset \mathbb{A}^n_k$ and ideal $\mathfrak{a}$ in A from Hilbert's Nullstellensatz and (2) of Problem 1. Hence it suffices to show the maps Z, I restricted on the prescribed domains map into the prescribed codomains.

(i) It suffices to show that I maps closed sets into radical ideals. We have seen this in (5) of Problem 1.

(ii) To show the second bijection, it suffices to show that I maps irreducible closed sets into prime ideals and Z maps prime ideals into irreducible closed sets. For this, we show that a closed set X is irreducible if and only if $I(X)$ is a prime ideal in A. First suppose X is irreducible, and assume for contradiction that $I(X)$ is not prime. Then there are polynomials $f, g \in A \setminus I(X)$ such that $fg \in I(X)$. Now consider the closed sets $V_1 := V(I(X) \cup \{f\})$ and $V_2 := V(I(X) \cup \{g\})$. Clearly those are contained in X, and not equal to X since $f, g \notin I(X)$. Also clear is that $X \subset V_1 \cup V_2$. Any $x \in X$ is a zero of $fg \in I(X)$, and hence it belongs to the union. Therefore $X = V_1 \cup V_2$, contrary to the assumption that X is irreducible.

Second, suppose $I(X)$ is prime. If X is not irreucible, there are closed sets $V_1 = Z(S_1), V_2 = Z(S_2)$ properly contained in X such that $X = V_1 \cap V_2$. Pick elements a_1 from $X \setminus V_1$ and a_2 from $X \setminus V_2$. Let $f \in S_1$ and $g \in S_2$. Then $f(a_1) \neq 0$ and $g(a_2) \neq 0$, which implies $f, g \notin I(X)$, but $fg \in I(X)$ since $X = V_1 \cup V_2$. This contradicts that $I(X)$ is prime.

Now we know that I maps irreducible closed sets into prime ideals. On the other hand, if S is a prime ideal in A then $Z(S)$ is a irreducible closed set since $I(Z(S)) = \overline{S} = S$ is prime ideal.

(iii) By Hilbert's Nullstellensatz, the maximal ideals in A are precisely the ones given by

$$I(P) = (x_1 - a_1, \cdots, x_n - a_n)$$

for some $P = (a_1, \cdots, a_n)$. This and (2) of Problem 1 gives the third assertion.

□

Convention : compact = compact + Hausdorff. quasi-compact = compact but not necessarily Hausdorff.

Proposition 16. Every Noetherian space is quasi-compact.

Proof. Use ACC for open sets. □

Projective Algebraic Sets. Recall that the projective space $\mathbb{P}^n$ is the quotient space $k^{n+1} - \{0\}/\sim$ where the equivalence relation $\sim$ is given by $x \sim \lambda y$ for all $\lambda \in k$. In the projective space, we only need to say about the zeros of *homogeneous* polynomials.

Definition 30. Let $S \subset k[x_0, \cdots, x_n]$ such that elements of S are homogeneous. Then define

$$Z(S) = \{x \in \mathbb{P}^n \mid f(x) = 0 \,\forall f \in S\} = Z(\langle S \rangle)$$

where $\langle S \rangle$ is a homogeneous ideal in A. Also define

$$I(Y) = \{f \in A_h \mid f(y) = 0 \,\forall y \in Y\}.$$

Then the properties that holds for affine algebraic sets such as $IZ(J) = \sqrt{J}$(Nullstellensatz), $ZI(J) = \overline{J}$ also holds in the projective algebraic sets.
Put $U_i = \{(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n \mid x_i \neq 0\} = \mathbb{P}^n - Z(x_i)$. Then

$$\mathbb{P}^n = \bigcup_{i=0}^{n} U_i.$$

Proposition 17 (Hartshorne 2.2)**.** $U_i \simeq \mathbb{A}^n$ homeo.

Hence $\mathbb{P}^n$ locally looks like $\mathbb{A}^n$. Also let X be a closed set in $\mathbb{P}^n$. Then we can write

$$X = \bigcup_{i=0}^{n} (X \cap U_i).$$

Note that $X \cap U_i$ is closed in U_i, hence homeomorphic to algebraic sets.
Let *variety* means the object that locally looks like affine algebraic sets. Everything will become clear once we use the language of *sheaf*.

Sheaf (in a category $\mathscr{C}$) on X(topological space).

Example 29 (Typical example)**.** $X : C^\infty$-manifold. U is open set in X. Then $C^\infty(U) := \{f : U \to \mathbb{R} \mid f \text{ is } C^\infty\}$.

A *presheaf* $\mathscr{O}$ (in $\mathscr{C}$) on X is a collection of $\mathscr{O}(U) \in \mathscr{C}$ for each open set $U \subset X$ together with (restriction) $\rho_V^U : \mathscr{O}(U) \to \mathscr{O}(V)$ if V is open in U(this means C^∞-ness is locally defined) such that

(0) $\mathscr{O}(\emptyset) = 0$;

(i) $\rho_U^U = id$;

(ii) $\rho_W^V \circ \rho_V^U = \rho_W^U$.

$\mathscr{O}$ is called a *sheaf* if elements in $\mathscr{O}(U)$ are "locally determined", i.e.,

(1) (Local identity) If $U = \bigcup_\alpha U_\alpha$ is an open covering, then $s \in \mathscr{O}(U)$, $S|_{U_\alpha} = 0$ for all α implies $s = 0$.

(2) (Gluing) Let $U = \bigcup_\alpha U_\alpha$ be an open covering and let $s_\alpha \in \mathscr{O}(U_\alpha)$ for each α. If $s_\alpha|_{U_\alpha \cap U_\beta} = s_\beta|_{U_\alpha \cap U_\beta}$ for all α, β, then there exists unique(by (1)) $s \in \mathscr{O}(U)$ such that $s|_{U_\alpha} = s_\alpha$.

Definition 31. Let X, Y be C^∞-manifolds. Then a map $\phi : X \to Y$ is C^∞ if for every open $V \subset Y$, we have map

$$C^\infty(X) \to C^\infty(\phi^{-1}(V)), \quad f \mapsto f \circ \phi|_{\phi^{-1}(V)}$$

Definition 32. (1) $(X, \mathscr{O}_X)$ is a *k-algebra(ringed)* space if X is a topological space and $\mathscr{O}_X$ is a sheaf of k-algebras on X.

(2) A morphism $\phi : (X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ in the category of ringed space is a continuous map $X \to Y$ which induces a k-algebra homomorphism $\phi^* : \mathscr{O}_Y(V) \to \mathscr{O}_X(\phi^{-1}(V))$, $f \mapsto f \circ \phi$ for every open set $V \subset Y$.

C^∞-manifold
Let X be a topological space. It is an n-dimensional manifold if for all $P \in X$, there is an open neighborhood U_α of p such that there is a homeomorphism $\phi_\alpha : U \to \phi_\alpha(U) \subset \mathbb{R}^n$. We call such pair (U_α, ϕ_α) a chart.
Given the local homeomorphisms from X to the Euclidean space $\mathbb{R}^n$, we can give X manifold structure by requiring the chart transitions to satisfy certain condition. We call X a *smooth(C^∞) manifold* if the chart transition maps are smooth, i.e., if $(U_\alpha, \phi_\alpha), (U_\beta, \phi_\beta)$ are two charts such that $U_\alpha \cap U_\beta \neq \emptyset$, then $\phi_\alpha \circ \phi_\beta^{-1}$ is C^∞ on $\phi_\beta(U_\alpha \cap U_\beta)$ and $\beta \circ \alpha^{-1}$ is C^∞ on $\phi_\alpha(U_\alpha \cap U_\beta)$.

Definition 33. Let $U \subset X$ be open. A map $f : U \to \mathbb{R}$ is C^∞ if it is locally represented by a smooth function, i.e., for each $p \in U$, there is a coordinate neighborhood $x \in U_\alpha \subset X$ such that $f \circ \phi_\alpha^{-1} : \phi_\alpha(U) \subset \mathbb{R}^n \to \mathbb{R}$ is C^∞.

Definition 34. Let X, Y be C^∞-manifolds. A map $\phi : X \to Y$ is *smooth* if it is locally represented by a smooth map on $\mathbb{R}^n$. That is, $\phi_\beta \circ \phi \circ \phi_\alpha^{-1}$ is C^∞ on $\phi_\alpha(U_\alpha)$ for all chart (U_α, ϕ_α)

$$\begin{array}{ccc} U_\alpha \subset X & \xrightarrow{\quad f \quad} & V_\beta \subset Y \\ \Big\downarrow{\scriptstyle \phi_\alpha} & & \Big\downarrow{\scriptstyle \psi_\beta} \\ \phi_\alpha(U_\alpha) \subset \mathbb{R}^n & \xrightarrow{\phi_\beta f \circ \phi_\alpha^{-1} \in C^\infty} & \psi_\beta(V_\beta) \subset \mathbb{R}^n \end{array}$$

Question : The coordinate chart map ϕ_α is smooth by tautology. If another atlas (V_β, ψ_β) gives a smooth structure on X, then is the previous chart map ϕ_α smooth with respect to the second smooth structure?

Notation. $U \subset X$ open. Denote $C_X^\infty(U) = \{f : U \to \mathbb{R} \mid f : C^\infty\}$. Hence C_X^∞ is a sheaf of k-algebra.

Proposition 18. $\phi : X \to Y$ is $C^\infty \iff$ for every $V \subset Y$ open, ϕ induces k-algebra homomorpihsm $\phi^* : C_Y^\infty(V) \to C_X^\infty(\phi^{-1}(V))$ by $g \mapsto g \circ \phi|_{\phi^{-1}(V)}$.

Proof. ($\Longrightarrow$) $C^\infty \circ C^\infty = C^\infty$.

($\Longleftarrow$) Note that the projection map is C^∞ and a map $f : \mathbb{R}^n \to \mathbb{R}^n$ is smooth if and only if each coordinate function is smooth. Put g be the projection maps.

□

Thus the category of C^∞ manifolds is a category of ringed space.

On could wish that given a sheaf $\mathcal{O}_X(U)$ of $\mathbb{R}$-valued functions, we might get C^∞ manifolds. But it could be the case that our sheaf might contain two functions which do not get along with each other. This statement is actually an emphasized one of that a C^∞-manifold is determined by its sheaf. Hence we might call the sheaf $\mathcal{O}_X^\infty$ of C^∞ manifold its *structure*.

Definition 35. Let $\mathcal{O}_X$ be a sheaf on X. Let $U \subset X$ be an open set. The *restriction sheaf* $\mathcal{O}_U = \mathcal{O}_X|_U$ is defined by $\mathcal{O}_U(V) = \mathcal{O}_X(V)$ for $V \subset U$ open.

Let X be a topological space.

(i) Given a sheaf $\mathcal{O}_X$ of $\mathbb{R}$-valued functions

(ii) X locally looks like open subsets of $\mathbb{R}^n$, i.e., $\forall P \in X$, $\exists (P \in) U \subset X$ open such that $(U, \mathcal{O}_X(U)) \simeq (B, C^\infty(B))$ as ringed space for some open subset $B \subset \mathbb{R}^n$.

HW 14. Show that the above two conditions are equivalent to "X is C^∞ manifold with $\mathcal{O}_X(U) \simeq C^\infty(U)$ for all open subset U."

HW 15. $C^\infty \circ C^\infty = C^\infty$, $\pi \in C^\infty$, mophism$\circ$morphism = morphism

Now we define the sturcture sheaf of algebraic sets.

Example 30. Let k be an algebraically closed field. $k^\times \to Z(xy-1) \subset \mathbb{A}^2_k$, $\alpha \mapsto (\alpha, \frac{1}{\alpha})$. The domain is Zariski open, where the range is Zariski closed.

Definition 36. Let X be a closed or open subset of $\mathbb{A}^n_k$, and U be an open subset of X. Define the sheaf of "regular functions" $\mathcal{O}_X$ as follows.

$$\begin{aligned} f : U \to k \text{ is regular} &\iff f \text{ is locally a rational polynomial function on } U \\ &\iff \forall P \subset U, \exists V \subset U \text{ open nbh of } P \text{ and } \exists g, h \in A \text{ s.t. } f(Q) = \frac{f(Q)}{g(Q)} \ \forall Q \in V,\ g(Q) \neq 0. \end{aligned}$$

Definition 37. Let $X \subset \mathbb{A}^n_k$ be an algebraic set. Then the pair $(X, \mathcal{O}_X)$ is called *affine variety*. More generally, $(Y, \mathcal{O}_Y)$ is an affine variety if $(Y, \mathcal{O}_Y) \simeq (X, \mathcal{O}_X)$ as ringed space for some algebraic set X.

Example 31. $X = \{(x,y) \in \mathbb{A}^2 \mid xy = 0\}$. Reducible. $U = \{(x,y) \in X \mid x \neq 0\} = \{(x,0) \mid x \neq 0\} \subset X$ is *affine open*. $V = \{(0,y) \mid y \neq 0\}$. On $U \cup V = X \setminus \{0\}$, we define

$$f(x,0) = x \text{ on } U,\ f(0,y) = \frac{1}{y} \text{ on } V.$$

Hence $f \in \mathcal{O}_{U \cup V}$.

Table for geometry and its hometown

Question : X : irreducible. Locally rational iff Globally rational? Seems to be a fundamental and hard question.
Given a geometry : always ask "what is the hometown? what is the structure sheaf?"

Recall that a topological space X is a smooth manifold if it locally looks like the hometown, $\mathbb{R}^n$, now considering the smooth maps altogether. We can view $\mathbb{R}^n$ as a smooth manifold with smooth maps defined on $\mathbb{R}^n$. Hence $(\mathbb{R}^n, C^\infty_{\mathbb{R}^n})$ is a ringed space. Then, given a ringed space (X, C^∞_X) of smooth manifold, is there "local isomorphism" between the two ringed spaces?
We can ask a question about the converse. Given a sheaf C^∞_X on the topological space X, can we define a smooth manifold structure on X?

Definition 38. Let $(X, \mathcal{O}_X)$, $(Y, \mathcal{O}_Y)$ be ringed space, where $\mathcal{O}_X$, $\mathcal{O}_Y$ are collectionof k-valued functions. Then a map $\phi : X \to Y$ is a *ringed space morphism* if

(i) ϕ is continuous and

(ii) $\forall V \subset Y$ open, the dual map $\phi^* : \mathscr{O}_Y(V) \to \mathscr{O}_X(\phi^{-1}(V))$ defined by $f \mapsto f \circ \phi|_{\phi^{-1}(V)}$ is a k-algebra homomorphism.

Proposition 19. Let X be a C^∞-manifold. Then the ringed space (X, C_X^∞) is locally isomorphic to the ringed space $(\mathbb{R}^n, C_{\mathbb{R}^n}^\infty)$, i.e., for each $p \in X$, there is an admissible coordinate chart (U_α, ϕ_α) containing p such that

$$\phi_\alpha : (U_\alpha, C_X^\infty|_{U_\alpha}) \longrightarrow (A, C_{\mathbb{R}^n}^\infty|_A)$$

is a ringed space isomorphism, where $A = \phi_\alpha(U_\alpha)$.

Proof. □

Conversely,

Proposition 20. Suppose a ringed space $(X, \mathscr{O}_X)$ locally looks like the "hometown", i.e., there is a local isomorphism from $(X, \mathscr{O}_X)$ to $(\mathbb{R}^n, C_{\mathbb{R}^n}^\infty)$. That is, for every $p \in X$, there is an open neighborhood $U \subset X$, open subset $A \subset \mathbb{R}^n$, and a homeomorpihsm $\phi : U \to A$ such that

$$\phi : (U, \mathscr{O}_X|_U) \longrightarrow (A, C_{\mathbb{R}^n}^\infty)$$

is a ringed space isomorphism. Then, X is a unique C^∞-manifold with $C_X^\infty = \mathscr{O}_X$ with the collection of all such pair (U, ϕ) being an atlas.

Proof. □

On the other hand, consider the affine space $\mathbb{A}^n$ with $\mathscr{O}_A$ the sheaf of regular functions for each algebraic set $A \subset \mathbb{A}^n$. Then we can think of a ringed space $(X, \mathscr{O}_X)$ which locally looks like this "hometown" $(\mathbb{A}^n, \mathscr{O}_{\mathbb{A}^n})$, i.e., for each $p \in X$, there is an open neighborhood $U \subset X$ such that we have the ringed space isomorphism

$$(U, \mathscr{O}_X|_U) \simeq (A, \mathscr{O}_A).$$

Think of the local ringed space isomorphism from given ringed space to the well-known "hometown" ringed space for geometry.
Recall directed system in a category $\mathscr{C}$.

Definition 39. I is a *directed index set* if

(i) : I is a poset

(ii) : If $i, j \in I$, then there is $k \in I$ such that $i, j \leq k$.

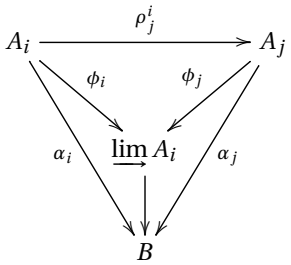
Definition 40. Let $\mathscr{C}$ be a category, and I a directed index set. For each indices $i \leq j$, let $\rho_i^j : A_j \to A_i$ be a morphism. Then we call $A = \left\{ A_i, \{\rho_i^j\}_{i \leq j} \right\}$ a *directed system* if

(i) : $\rho_i^i = id$

(ii) : $i \leq j \leq k \Rightarrow \rho_i^j \circ \rho_j^k = \rho_i^k$.

Example 32 (Typical example)**.** X: smooth manifold. $C^\infty(U) = \{f : U \xrightarrow{C^\infty} \mathbb{R}\}$. $\rho_V^U : C^\infty(U) \to C^\infty(V) : f \mapsto f|_V$: restriction onto V if $U \subset V$. Germ. $f = f|_V$. Considering two images identical $\leftrightarrow$ quotient.

Definition 41 (Direct limit)**.**



Existence of direct limit in Mod_R. Since it is the dual of the inverse limit, which was a subset of the categorical product, the direct limit must be the image of coproduct. That is, the "maximal quotient module" of the coproduct $\bigoplus_i A_i$ for which the above diagram for direct limit commutes.

$$A = \varinjlim A_i = \bigoplus_i A_i / \langle \iota_j \rho_j^i a_i - \iota_j a_i \rangle_{R\text{-submodule}}$$

Definition 42. $(X, \mathcal{O}_X)$: ringed space. $\mathcal{O}_X(U)$ is a k-algebra of k-valued functions on U, where the operations are given by the operations in k.(think of the typical example of smooth manifolds with smooth maps). Define an equivalence relation on $\mathcal{O}_X$ as follows: for fixed point $P \in X$, consider $f \in \mathcal{O}_X(U)$ and $g \in O_X(V)$ where U, V are some open neighborhoods of P. We define relation

$$f \sim_P g$$

if $f = g$ one some neighborhood W of P that is contained in $U \cap V$. This defineds an equivalence relation, and each equivalence class $[f]_P$ is called the *germ at* P. The set of all germs at P is called the *stalk at* P and denoted $\mathcal{O}_P$.

Roughly speaking, the germ $[f]_P$ at P is the collection of all functions $g \in \mathcal{O}_X$ that is locally the same as f near P. When considering the stalk $\mathcal{O}_P$, we only considers the local behavior of functions f of the sheaf $\mathcal{O}_X$. One can predict that the stalk might be given as a local ring

HW 16. $[f+g] = [f] + [g]$, $[fg] = [f][g]$. That is, $\mathcal{O}_p$ has a quotient ring structure.

Theorem 14. Show that $\mathcal{O}_P \simeq \varinjlim_{P \in U \subset X} \mathcal{O}_X(U)$ as abelian groups, under the map $\Phi : [f]_P \mapsto \phi_U(f)$, i.e.,

$$[f]_P \longmapsto \overline{(0, \cdots, 0, f, 0, \cdots, 0)}$$

where $f \in \mathcal{O}_X(U)$.

Proof. Let $f \sim_P g$, where $f \in \mathcal{O}_X(U)$ and $g \in \mathcal{O}_X(V)$. We need to show $\phi_U(f) = \phi(V)(g)$. Since $f \sim_P g$, there is an open neighborhood W of P contained in $U \cap V$ such that $f = g$ on W. Denote $h = f|_W = g|_W \in \mathcal{O}_X(W)$. Hence we have

$$\phi_U(f) = \phi_W(f|_W) = \phi_W(h) = \phi(g|_W) = \phi_V(g).$$

This shows the map Φ is well-defined. That Φ is an additive group homomorphism is clear, since

$$\Phi([f]_P + [g]_P)(x) = (\phi_U(f) + \phi_V(g))(x) = \phi_U(f)(x) + \phi_U(g)(x)$$

for every $x \in U \cap V$. It remains to show the surjectivity. This follows from the following proposition. Assuming it, indeed, if $f \in \varinjlim_{P \in U} \mathcal{O}_P(U)$, then we may write $f = \phi_U(g)$ for some $g \in \mathcal{O}_X(U)$. Then $f = \Phi([g]_P)$, and therefore Φ is surjective. □

Proposition 21. Let $A_i \in Mod_R$ and $a \in \varinjlim A_i$. Then $\exists j \in I$, $\exists a_j \in A_j$ such that $\phi_j a_j = a$.

Proof. Let $a = \overline{(0, \cdots, a_{i_1}, \cdots, a_{i_2}, \cdots, a_{i_3}, \cdots 0)}$. Since the index set I is a directed set, there is $j \geq i_1, i_2, i_3$. Put

$$\begin{aligned} b_1 &= \overline{(0, \cdots, 0, \rho_j^{i_1} a_{i_1}, 0, \cdots, 0)} \\ b_2 &= \overline{(0, \cdots, 0, \rho_j^{i_2} a_{i_2}, 0, \cdots, 0)} \\ b_2 &= \overline{(0, \cdots, 0, \rho_j^{i_2} a_{i_2}, 0, \cdots, 0)}. \end{aligned}$$

Then we have

$$\begin{aligned} b_1 + b_2 + b_3 &= \overline{(0, \cdots, 0, a_{i_1}, 0, \cdots, 0)} + \overline{(0, \cdots, 0, a_{i_2}, 0, \cdots, 0)} + \overline{(0, \cdots, 0, a_{i_3}, 0, \cdots, 0)} \\ &= a \end{aligned}$$

□

Proposition 22. (1) $a_k \in A_k$, $\phi_k a_k = 0 \Longrightarrow \exists \geq k$ such that $\rho_l^k a_k = 0$.

(2) $\phi_i a_i = \phi_j a_j$ where $a_i \in A_i$, $a_j \in A_j \Longleftrightarrow \exists k \geq i, j$ such that $\rho_k^i a_i = \rho_k^j a_j$.

Proof. (1) Obvious in stalk. "if locally identical, then still identical if restricted".

(2) Try for 1 hour, and refer to Babakhanian.

□

HW 17. Details for the proof of theorem 14.

Note that the coproduct of two k-algebras is a tensor product. But arbitrary coproduct of k-algebras might not exists. Hence the similar construction of the direct limit in the category of R-modules as the image of coproduct does not work in the category of k-algebras. However, there is a clever detour for this.

Theorem 15. Direct limit exists in the category of k-algebra.

Proof. Let A be the direct limit of A_i in the category of k-modules. Need to define multiplication. Let $a, b \in A$. Then $a = \phi_i a_i$, $b = \phi_j a_j$ for some indices i, j and $a_i \in A_i$, $a_j \in A_j$. Let $k \geq i, j$. Then define

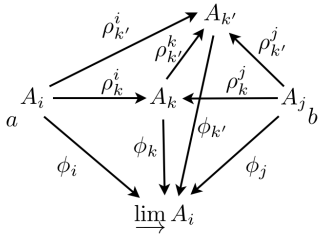
$$a \cdot b := \phi_k[(\rho_k^i a_i) \cdot (\rho_k^j a_j)].$$

where the product $(\rho_k^i a_i) \cdot (\rho_k^j a_j)$ takes place in A_k. We need to ensure following points. In vector notation, if

$$a \cdot b = (0, \cdots, 0, a_i, 0, \cdots, 0) \cdot (0, \cdots, 0, a_j, 0, \cdots, 0) = (0, \cdots, \cdots, 0, a_i a_j, 0, \cdots, 0)$$

(1) Well-defined?

We need to show the product $a \cdot b$ does not depend on the choice of k and also of the choice of a_i, a_j. Use the notation $a \cdot_k b$ temporarily. Let $k, k' \geq i, j$. We may assume $k' \geq k$. We need to show $a \cdot_k b = a \cdot_{k'} b$. This follows from the commutative diagram below and the fact tha $\rho^k_{k'}$ is a k-algebra homomorphism.



(2) ϕ_k is a k-algebra homomorphism?

Clear from the construction.

(3) $\varinjlim A_i$ is a k-algebra?

Distributivity. Check.

□

Theorem 16. $\mathcal{O}_P \simeq \varinjlim_{P \in U \subset X} \mathcal{O}_X(U)$ as k-algebra.

T.A. Springer, Linear Algebraic Groups, Chapter 1.
variety + group $\subset GL_n(k)$.
J.E. Humphreys, Linear Algebraic Groups A.Borel, Linear Algebraic Groups

Example 33. $k^* \longleftrightarrow Z(xy-1) \subset \mathbb{A}^2$ by $\alpha \longrightarrow (\alpha, \frac{1}{\alpha}) \subset \mathbb{A}^2$. Isomorphic as locally ringed space.

Example 34. $f(x_1, \cdots, x_n) \subset k[x_1, \cdots, x_n]$. $\mathbb{A}^n - Z(f) \approx Z(f(x_1, \cdots, x_n)x_{n+1} - 1)$: closed in $\mathbb{A}^{n+1}$. LHS is open in $\mathbb{A}^n$, affine open subset.

$$\begin{aligned} k[Z(f \cdot x_{n+1} - 1)] &= k[x_1, \cdots, x_{n+1}]/(f \cdot x_{n+1} - 1) \\ &\approx k[x_1, \cdots, x_n]_f. \end{aligned}$$

Let X be an affine variety in $\mathbb{A}^n$.(algebraic set) $f \in k[X] = A/I(x)$. Define $D(f) = X - V(f)$.

HW 18. $\{D(f) \mid f \in k[X]\}$ is a base for the topology of X.

Proof. We need to show that any open subset in X is a union of the sets of the form $D(f)$. Let $U = X - Z(f_1, \cdots, f_r)$ be any open subset of X, for some polynomials $f_1, \cdots, f_r \in k[x_1, \cdots, x_n]$. Observe that

$$\begin{aligned} U &= X - Z(f_1, \cdots, f_r) \\ &= X \cap \left(\bigcap_{i=1}^{r} Z(f_i) \right)^c \\ &= X \cap \left(\bigcup_{i=1}^{r} Z(f_i)^c \right) \\ &= \bigcup_{i=1}^{k} (X \cap Z(f_i)^c) \\ &= \bigcup_{i=1}^{k} (X - Z(f_i)) = \bigcup_{i=1}^{k} D(\overline{f_i}) \end{aligned}$$

where $\overline{f_i}$ is image of f_i under the cannonical projection $k[x_1, \cdots, x_n] \to k[X]$. □

Note that

$$D(f) \approx \{(x_1, \cdots, x_n, x_{n+1}) \in \mathbb{A}^{n+1} \,\big|\, (x_1, \cdots, x_n) \in X,\, f(x_1, \cdots, x_n) x_{n+1} = 1\}$$

is a closed subset of $\mathbb{A}^{n+1}$. Then

HW 19. $k[D(f)] \approx k[X]_f$.

Proof. Let $X = Z(f_1, \cdots, f_k)$ for some polynomials $f_1, \cdots, f_k \in k[x_1, \cdots, x_n]$. Then

$$k[D(f)] = k[x_1, \cdots, x_{n+1}] / (f_1, \cdots, f_k, f \cdot x_{n+1} - 1).$$

We show the map

$$\phi : k[x_1, \cdots, x_{n+1}] \longrightarrow k[X]_f, \quad g(x_1, \cdots, x_{n+1}) = g(x_1, \cdots, x_n, 1/f(x_1, \cdots, x_n))$$

is a surjective ring homomorphism with kernel $(f_1, \cdots, f_k, f \cdot x_{n+1} - 1)$. That the kernel is as claimed is clear. That ϕ is a ring homomorphism is also clear since ϕ can be viewed as an evaluation homomorphimsm $x_{n+1} \mapsto 1/f$. The surjectivity is also clear, since for any $g/f^r \in k[X]_f$, we have $\phi(g \cdot x_{n+1}^r) = g/f^r$. Hence we have $k[D(f)] \approx k[X]_f$ as desired. □

Theorem 17. Let $(X, \mathcal{O}_X)$ be affine variety. Then

(a) $\mathcal{O}_X(X) \approx k[X]$

(b) $P \in X$. $\mathcal{O}_P \approx k[X]_{m_P}$ where

$$m_P = \{f \in k[X] \mid f(P) = 0\}$$

is a maximal ideal in $k[X]$. (That's why it is called "localization")

Proof. (a) Define $k[X] \to \mathcal{O}_X(X)$, $f \mapsto f$. Surjective?

Surjectivity proof

(1) Hartshorne (X : irreducible)

(2) T.A. Springer, p.8. Elementary proof (not necessarily for X irreducible) (compare with Hartshorne pp. 71-72 "scheme")

(b) Germ $\mathcal{O}_P \longleftrightarrow k[X]_{m_P}$ by

$$[k/h, U] \longleftrightarrow k/h$$

for some $h, k \in k[X]$ with $h(P) \neq 0$.

□

Question. Concerning (a), why didn't we defined the regular functions globally as follows?

$$\mathcal{O}_X(U) = \{g \mid g : U \to k \text{ is a polynomial }\}$$

No counter example in affine variety. Maybe some in projective.
We ommit the dimension of algebraic varieties. Similar assertion holds for projective varieties.

Definition 43. Let $(X, \mathcal{O}_X)$ be a ringed space, where $\mathcal{O}_X$ is a sheaf of k-valued functions. It is called a *prevariety* if it locally looks like our hometown(affine variety), i.e., $\forall P \in X\ \exists P \in U \subset X$ open such that $(U, \mathcal{O}_X|_U) \approx (Y, \mathcal{O}_Y)$ as rined space for some algebraic set $Y \subset \mathbb{A}^n$ with the structure sheaf $\mathcal{O}_Y$.

Definition 44. A ringed spcae $(X, \mathcal{O}_X)$ is a C^∞-manifold if it is locally looks like $(\mathbb{R}^n, C^\infty_{\mathbb{R}^n})$ and X is Hausdorff, 2nd countable.

Definition 45. A ringed space $(X, \mathcal{O}_X)$ is called an *algebraic variety* if it is a prevariety + "separation axiom". (note that even our hometown-affine variety- is not Hausdorff.)

Definition 46. $(X, \mathcal{O}_X)$ is an *affine variety* if it is the hometown in $\mathbb{A}^n$, and *projective variety* if it is the hometown in $\mathbb{P}^n$.

Theorem 18. $(X, \mathcal{O}_X)$: projective variety. Then $\mathcal{O}_X(X) \approx k$.

Note :

$$\text{functor : Affine Variety} \longrightarrow \text{finitely generated reduced k-Alg}$$

$$(X, \mathcal{O}_X) \longmapsto k[X] = A/I(X)$$

Given $\phi : X \to Y$, define $\phi^* : k[Y] \to k[X]$ $f \mapsto f \circ \phi$. Anti-equivalence.

Theorem 19. X any pre variety, Y : affine variety. Then

$$\mathrm{Mor}(X, Y) \xrightarrow{\sim} \mathrm{Hom}_{k-alg}(k[Y], \mathcal{O}_X(X)).$$

Proof. Given $h \in \mathrm{Hom}_{k-alg}(k[Y], \mathcal{O}_X(X))$, define $h \mapsto \psi$ by

$$\psi(P) = (\zeta_1(P), \cdots, \zeta_n(P))$$

where $\zeta_i = h(\overline{x_i})$ for $x_i \in k[x_1, \cdots, x_n]$, $\overline{x_i} \in k[x_1, \cdots, x_n]/I(Y)$. We need to check $\psi(P) \in Y$, i.e., $f(\psi(P)) = 0$ for all $f \in I(Y)$. Obseve

$$f(\zeta_1(P), \cdots, \zeta_n(P)) \overset{*}{=} h(f(\overline{x_1}, \cdots, \overline{x_n}))(P) \overset{**}{=} 0$$

□

HW 20. Verify $*$ and $**$ for $f(x_1,x_2)=x_1^2x_2+x_1+3$, h:k-alge hom.

Theorem 20. Category of affine variety = Category of finitely generated reduced k algebra

HW 21. Let X,Y be algebraic sets. $\phi: X\to Y$ morphism iff ϕ : polyomial map. regular = poly.

Proposition 23. $k[X]\approx\mathcal{O}(X)$.

Proof. Define map $\phi: k[X]\to\mathcal{O}(X)$ by $f\mapsto f$. surjectivity?
$\forall f\in\mathcal{O}_X(X)$ for all $x\in X$ there is U_x : nbh of x, $g_x,h_x\in k[X]$ such that $f|_{U_x}=\frac{g_x}{h_x}$.
$\{D_f\}$: basis. WMA $U_x=D(a_x)$, $a_x\in j[X]$.
$D(a_x)\subset D(h_x)\Rightarrow Z(a_x)\supset Z(h_x)$.
Hence $\sqrt{(a_x)}=IZ(a_x)=\subset IZ(h_x)=\sqrt{(h_x)}$. Thus $a_x\in\sqrt{(h_x)}$.
Hence there is $h'_x\in k[X]$, $n_x\geq 1$ such that $a_x^{n_x}=h_xh'_x$.
$f|_{U_x}=\frac{g_xh'_x}{a_x^{n_x}}$, $D(a_x)=D(a_x^{n_x})$.
We set $a_x^{n_x}\mapsto a_x$, $g_xh'_x\mapsto g(x)$. (WMA $h_x=a_x$).
Since X is quasi-compact, $\exists h_1,\cdots h_s\in k[X]$ such that $\{D(h_i)\}$ covers X.
$f|_{D(h_i)}=\frac{g_i}{h_i}$, $\exists g_i\in k[X]$.
$\frac{g_i}{h_i}=\frac{g_j}{h_j}$ on $D(h_i)\cap D(h_j)$, $h_ih_i=0$ on $X\setminus D(h_i)\cap D(h_j)$.
$h_ih_j(g_ih_j-g_jh_i)=0$.
$\{D(h_i^2)\}$ covers X.
Thus $Z(\{h_i^2\})=\bigcap_{i=1}^s Z(\{h_i\})=0$
$\sqrt{(h_1^2,\cdots,h_s^2)}=IZ(\{h_i^2\})=k[X]$.
$1^n\in(h_1^2,\cdots h_s^2)$. Thus $(h_1^2,\cdots h_s^2)=k[X]$.
$\exists b_i\in k[X]$ s.t. $\sum_{i=1}^s b_ih_i^2=1$.
$\forall x\in D(h_i)$, $h_j^2\sum_{i=1}^s b_ig_ih_i(x)=\sum_{i=1}^s b_ih_i^2h_jg_j=h_j^2f$.
$f=\phi(\sum_{i=1}^s b_ig_ih_i)$. Surjective.

□

HW 22. Let R be a ring, and $\mathfrak{a}\subset R$ an ideal. Show that

$$\sqrt{a}=\bigcap_{\substack{\mathfrak{a}\leq P\\ P:\text{PI in R}}} P.$$

8 SCHEME LANGUAGE

Product of Affine varieties. We want $\mathbb{A}^n \times \mathbb{A}^m \approx \mathbb{A}^{n+m}$ homeo. Let $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ be closed subsets. Then $X \times Y \subset \mathbb{A}^n \times \mathbb{A}^m$ is a closed subset, and we want to identify $\mathbb{A}^n \times \mathbb{A}^m \approx \mathbb{A}^{n+m}$. Note that

$$\{(x_1, \cdots, x_n, y_1, \cdots, y_m) \in \mathbb{A}^{n+m} \mid f(x_1, \cdots, x_n) = 0,\ g(y_1, \cdots, y_m) = 0 \text{ for all } f \in I \text{ and } g \in J\}$$

Now we define the product topology of $X \times Y$ as the induced topology in $\mathbb{A}^{n+m}$.
Let $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ be affine prevarieties;

$$X = Z(f_1(x_1, \cdots, x_n), \cdots), \quad Y = Z(g_1(y_1, \cdots, y_m), \cdots).$$

Define

$$X \times Y = \{(x, y) \in \mathbb{A}^{n+m} \mid f_i(x) = 0\ g_j(x) = 0 \text{ for all } i, j\ \}$$

Then we claim that $X \times Y$ is a categorical product in $AffVar$. We need to show that

(1) the maps $p : X \times Y \to X$, $q : X \times Y \to Y$ are morphisms. This is clear since they are polynomial map.

(2) the commuting diagram.

Note that (1) implies that the topology on $X \times Y$ is finer than the product topology

Example 35. $\mathbb{A}^1 \times \mathbb{A}^1 \approx \mathbb{A}^2$. If LHS is product topology, closed set=finite set. But RHS has more closed sets.

$k[X \times Y] \approx k[X] \otimes_k k[Y]$.

Note 3. Let X be a topological space. Then X is Hausdorff iff the diagonal $\Delta(X)$ is a closed subset of $X \times X$("diagonal is closed")

Recall that a prevariety is a ringed space that is locally homeomorphic to $\mathbb{R}^n$.

Definition 47 (Hausdorff separation axiom)**.** A prevariety X is a variety iff it satisfies the Hausdorff separation axiom, i.e., $\Delta(X) \subset X \times X$ is closed, where $X \times X$ has Zariski topology.

Theorem 21. There exists categorical product in the category of prevariety.

Proof. $X = \bigcup_{i=1}^r U_i$, $Y = \bigcup_{j=1} U_j$ where U_i, V_j are affine open. We know the categorical product $U_i \times U_j$. Then define

$$X \times Y = \bigcup_{i,j} U_i \times U_j.$$

"Glue together". □

Note 4. Let X be a nice(locally compact Hausdorff) space. Then X is compact iff the proejction map

$$X \times Y \to Y$$

is closed map for all (...) space Y.

Definition 48. Let X be a variety. We call X *complete* if for all variety Y, the projection map

$$X \times Y \to Y$$

is closed map.

Theorem 22. Affine algebraic group(affine var and alg gp) is isomorphic(as gp and aff var.) to a Zariski closed subgroup of $GL_n(k)$ for some n.

Proof. Omitted. □

Thus we call affine algebraic group a *linear algebraic group*.
Exception : elliptic curves. lives in projective space
Know $X \times Y$: categorical product of $X \times Y$ in AffVar. Thus $k[X \times Y]$ is a coproduct of $k[X]$ and $k[Y]$ in f.g. reduced k-Alg. Thus $k[X \times Y] \approx k[X] \otimes k[Y]$.

Scheme. Hometown : A : ring. Spec A = the set of prime ideals of $A \supset$ maximal ideals($\leftrightarrow$ points)
Define structure sheaf $(SpecA, \mathcal{O})$.
Locally ringed space. Look up for definitions. (Harshorne Ch2.)
Sturcture sheaf $\mathcal{O}(U)$ is a ring. Up until now it was a k-algebra. Recall that a ring is a $\mathbb{Z}$-algebra.
We want to reduce the hypothesis on the algebraically closedness of k. So searched for alternative languages.
Now fix a ring k. We can lift up or restrict the theory itself. So suffices to do for algbraically closed field.
Question : Why Spec A? Why locally ringed space?
Scheme language is not the unique solution. (a better one)
Now its a normal science. It has been a paradigm.
Up until now $\phi : X \to Y$ is a morphism if (by def) it induces k-algebra homomorphism if $\phi^* : \mathcal{O}_Y(V) \to \mathcal{O}_X(\phi^{-1}(V))$ by $g \mapsto g \circ \phi|_{\phi^{-1}(V)}$.
in locally ringed space, $(\phi, \phi^\#)$, $\phi^\# : \mathcal{O}_Y \to \mathcal{O}_X$. ϕ and $\phi^\#$ is independent. totally different two data.

Example 36. $SL_n(R) = \{(r_{ij}) \in R^{n^2} \mid \det(r_{ij}) - 1 = 0\}$, $E(R) = \{(r,s) \in R^2 \mid s^2 - 5r^3 + \sqrt{2}r - 1\}$. We want to understant SL_2, E as functors. $-5, \sqrt{2} \in k$: ring.
To define polynomials R must be a k-algebra.
Thus it is a functor from k-algbra to Set.

Category of dreams. A *dream* F is a covariant functor k-alg $\to Set$. It satiesfies following properties.

(i) I : index set, X_i : indeterminate ($i \in I$), $T \subset k[\{X_i\}_{i \in I}]$.

$F(R) = \{(r_i) \in \prod_{i \in I} R \mid f((r_i)) = 0 \forall f \in T\}$.

F : a covariant functor? Need to check $\phi : R \to S$ k-alg homomorphism. $F(R) \to F(S)$.

(We assume everything is commutative. hom : $1 \mapsto 1$.)

$(r_i) \mapsto (\phi r_i)$.

F maps id to id

preserves composition

Object is Functor!

Definition 49. Let $\mathscr{C}$, $\mathscr{D}$ be categories. $\mathscr{F}(\mathscr{C},\mathscr{D})$: functor category. An object is a functor $F : \mathscr{C} \to \mathscr{D}$. $Mor_{\mathscr{F}(\mathscr{C},\mathscr{D})}(F,G) = NatTransf(F,G)$ natrual transformation = $\{\eta_X\}$.

Fundamental Question : $NatTransf(F,G)$ is a set? Not necessarily.
Ob can be more than a set, while Mor must be a set. Why?
Foundation of Category theory. One can avoid the axiom of choice.
If $\mathscr{C}$, $\mathscr{D}$ are small categories, then everything is a set.
the category of gp is not a small category. But if we consider the isomorphism classes, then it can be a small category. Really? for cyclic groups we knew the classification.
$F_{I,T}(R) = \{(r_i) \in \prod_{i\in I} R \mid f((r_i)) = 0 \forall f \in T\}$. Hence the "dreams" can be at most $\#set$ many.
We may only consider small categories.
The category of dreams is a full subcategory of $\mathscr{F}(k-Alg, Set)$.
The category of dreams = representable functors(= equivalent to Hom functor)

Definition 50. $F : k-Ale \longrightarrow Set$ is a representable functor if $F \approx \mathrm{Hom}_{k-Alg}(A,-)$ for some k-algebra A, where the isomorphism is in the functor category = natural equivalence. "F is represented by A".

$$\text{Category of representable functors} \underset{\text{Yoneda Lemma}}{\overset{anti-equiv}{\longleftarrow}} k-Alg \xrightarrow[anti-equiv]{} \text{Affine Schemes over } k$$

Example 37. R:ring. $Spec(R)$ is an affine scheme over Z. $k = \mathbb{Z}$.

There is a geometry, locall structure in the category of affine schemes over k. From the equivalence, we can consider geometric structure for each dream.

Definition 51. $G : k-Alg \to Set$ is a representable functor if and only if $G \approx \mathrm{Hom}_{k-Alg}(A,-)$ for some k-algebra A.

Theorem 23. The category of dreams and the category of representable functors is isomorphic.

Notation : Hom = Hom_{k-alg}

Proof. Define $F \longmapsto \mathrm{Hom}(A,-)$ where $A = k[(X_i)]/\langle T\rangle$. □

Example 38. $\mathbb{G}_a$: the additive group. $\mathbb{G}_a(R) = R \overset{set}{\approx} \mathrm{Hom}(k[X], R)$

Example 39. $\mathbb{G}_m$: the multiplicative group. $GL_1(R) = \mathbb{G}_m(R) = R^\times \overset{set}{\approx} \mathrm{Hom}(k[X,Y]/\langle XY-1\rangle, R)$ $GL_n(R) \approx \mathrm{Hom}(k[\{X_{ij}\}]/\langle \det(X_{ij}) - 1\rangle, R)$

Category of dreams = Category of representable functors

Example 40. dream F : $F(R) = \{r \in R \mid r = 0\} \leftrightarrow A = \frac{k[X]}{\langle X\rangle}$
dream G :
dream F : $F(R) = \{r \in R \mid r^2 = 0\} \leftrightarrow C = \frac{k[X]}{\langle X^2\rangle}$
and A, B are not isomorphic. Thus $Spec(A) \neq Spec(C)$. $F \neq H$ in general. There could be

$$\begin{array}{ccc} \text{Big dreams} = & \text{representable functors} \\ \cup & \cup \\ \text{dreams} = & \text{Hom functors} \end{array} \tag{8.1}$$

Lemma 2 (Yoneda)**.**

$$\begin{array}{rcl} \mathrm{Hom}_{k-alg} & \xrightarrow{1-1} & \mathrm{Mor}(\mathrm{Hom}(A,-),\mathrm{Hom}(B,-)) \\ \psi & \longmapsto & [\psi] \\ \Phi_A(id_A) & \longleftarrow & \Phi \end{array}$$

Category of sheaves on X. An object = a sheaf on X. $\phi : \mathscr{F} \to \mathscr{G}$ is a sheaf morhism if and only if we have the commutative diagram for each open sets $V \subset U \subset X$.

$$\begin{array}{ccc} \mathscr{F}(U) & \xrightarrow{\phi_U} & \mathscr{G}(U) \\ \downarrow{\scriptstyle \rho_V^U} & & \downarrow{\scriptstyle \rho_V^U} \\ \mathscr{F}(V) & \xrightarrow{\phi_V} & \mathscr{G}(V) \end{array}$$

Notation. $k = \mathbb{Z}, A, R, S, \cdots$:ring.

Definition 52. $\mathrm{Spec}(R) = \{\mathfrak{p} \mid \text{prime ideals of } R\}$

Example 41. $\mathrm{Spec}(\mathscr{C}[X]) = \{\langle p(x)\rangle \mid p\text{:irreducible}\} \cup \{0\}$

why including the zero ideal is good? future study.
Let $\mathfrak{a}$ be an ideal in R. We define closed sets in R as the sets

$$V(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Spec\ R} \mid \mathfrak{a} \subset \mathfrak{p}\}.$$

This gives a topology on Spec$R$.

Example 42. $V(R) =, V(0) = \mathrm{Spec}(R)$, $V(\mathfrak{a}\cdot\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$, $V(\sum_i \mathfrak{a}_i) = \bigcap_i V(\mathfrak{a}_i)$

Definition 53.

$$\mathscr{O}_{\mathrm{Spec}(U)} = \left\{ f : U \to \bigsqcup_{\mathfrak{p}\in\mathrm{Spec}(R)} R_{\mathfrak{p}} \;\middle|\; \forall \mathfrak{p} \subset U\ \exists W \subset U\ \exists a, b \in R \text{ s.t. } f(q) = \frac{a}{b} \in R_q\ \forall q \in W \right\}$$

Definition 54. $(\mathrm{Spec}(R), \mathscr{O}_{\mathrm{Spec}(U)})$: Spectrum. $(X, \mathscr{O}_X)$ is a spectrum if and only if $(X, \mathscr{O}_X) \overset{LRS}{\approx} (\mathrm{Spec}(R), \mathscr{O}_{\mathrm{Spec}(R)})$

$\{ring\} \to$ Spectrums.

$$\begin{array}{rcl} \mathrm{Hom}_{\mathbb{Z}-alg} & \xrightarrow{1-1} & \mathrm{Mor}_{LRS}(\mathrm{Spec}(R), \mathrm{Spec}(S)) \\ f : S \to R & \longmapsto & (\mathfrak{p} \mapsto f^{-1}(\mathfrak{p})) \end{array}$$

Define LRS so that the image of the above map is the morphism of LRS
Locally Ringed Space $(X, \mathscr{O}_X)$.

Definition 55. Let $f : X \to Y$ be a continuous map. For all open subset $V \subset Y$, we define

$$(f_*\mathscr{O}_X)(V) := \mathscr{O}_Y(f^{-1}(V))$$

: direct image sheaf.

Check : $f_*\mathscr{O}_X$ is a sheaf.

Definition 56. Let $k=\mathbb{Z}$. X is a topological space, $\mathscr{O}_X$ a sheaf of rings. Assume for all $P\in X$, $\mathbb{O}_P=\varinjlim_{P\subset U\subset X}\mathscr{O}_X(U)$: local ring. Then a map

$$(\phi,\phi^{\#}):(X,\mathscr{O}_X)\longrightarrow(Y,\mathscr{O}_Y)$$

is a *locally ringed space morphism* if

(i) $\phi: X\to U$ is continuous;

(ii) $\phi^{\#}:\mathscr{O}_Y\to\phi_*\mathscr{O}_X$ is a sheaf morphism

(iii) $\phi^{\#}_P:\mathscr{O}_{Y,\phi(P)}\to\mathscr{P}_{X,P}$ is a local homomorphism for all $P\in X$

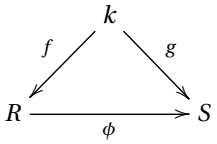
Definition 57. Let A,B be local rings. $g:A\to B$ is a *local homomorphism* if $g^{-1}(\mathfrak{m}_B)=\mathfrak{m}_A$.

Why the definitions are so complicated? Unique reason : "dream".

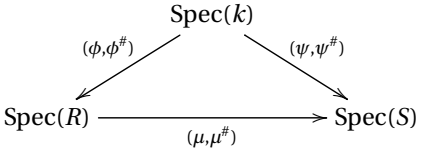
Definition 58. $(X,\mathscr{O}_X)$ is an *affine scheme* over $\mathbb{Z}$ if $(X,\mathscr{O}_X)\overset{LRS}{\approx}(\mathrm{Spec}(A),\mathscr{O}_{\mathrm{Spec}(A)})$.

$$\mathrm{Hom}_{k-alg}(B,A)\overset{1-1}{\longleftrightarrow}\mathrm{Mor}_{LRS}(\mathrm{Spec}(A),\mathrm{Spec}(B))$$
$$\mu\longmapsto\Psi(\mu),\quad \Psi(\mu)(\mathfrak{p})=\mu^{-1}(\mathfrak{p}).$$

to make the dream of making the correspondence Ψ bijective.
Now we are done for $k=\mathbb{Z}$.
Category of k-algebra.(Lang) Obejects : $(k\xrightarrow{f}R)$ ring homomorphism, Morphisms : commutative triangle



Fix a ring k. Given a k-algebra $k\overset{ring}{\to}R$. Get $\mathrm{Spec}(k)\overset{LRS}{\leftarrow}\mathrm{Spec}(R)$; this is called an affine scheme over k. Morphisms : commutative triangle



Definition 59. Scheme over k = locally affine scheme over k.

Recall $\mathscr{O}(X)(X)=k[X]$. Similarly $\mathscr{O}_{\mathrm{Spec}(R)}(\mathrm{Spec}(k))\simeq R$.
Hartshorne Proposition 2.6(p.78)
Let k be an algebraically closed field. functor $t:Var\to Sch_k$ full an faithfull.

REFERENCES

[1] Thomas Lang, *Algebra*. Springer, 3rd ed.

[2] Nathan Jacobson *Basic Algebra 2*. W. H Freeman and company

[3] Z. I. Borevich, I. R. Shafarevich *Number Theory*. Academic Press

[4] Willam Fulton *Algebraic Geometry*.

[5] Klaus Hulek *Elementary Algebraic Geometry*.

[6] Robin Hartshonre *Algebraic Geometry*. Springer