Basics on commutative algebra

August 2014

1 Modules

Rings are supposed to be commutative and unitary.

Definition 1.1. 1. Let A be a ring, an A-module M is a commutative group M endowed with a product

$$\begin{array}{rccc} A \times M & \to & M \\ (a, x) & \mapsto & a * x \end{array}$$

such that

(a) associativity:

$$a, b \in A, x \in M, a * (b * x) = (ab) * x$$

(b) distributivity:

$$(a+b) * x = a * x + b * y, y \in M$$

(c)
$$1_A * x = x \iff 0_A * x = 0_M, (-1)_A * x = -x$$

2. We define the expression ax for $a \in A$ and $x \in M$ as

 $ax \equiv a * x$

- 3. If $f: M \to N$, (M, N are A-modules) is a group homomorphism and f(a * x) = a * f(x), $\forall a \in A$, $\forall x \in M$, then f is called a module homomorphism
- 4. A submodule of M is a subgroup N such that $ax \in N$, $\forall x \in N$, $\forall a \in A$
- 5. let $S \subset M$ subset, a submodule of M generated by S is the smallest submodule of M containing S. It is also equal to

$$\bigcap_{N \text{ submodule containing } S} N = \{a_1x_1 + ...a_nx_n | a_1, ..., a_n \in A, x_1, ..., x_n \in S, n \text{ varies}\}$$

Exercise 1.2. All vector spaces are modules. Every ring is a module over itself, and its submodules are precisely its ideals. Modules over \mathbb{Z} are exactly the abelian groups up to isomorphism.

Example 1.3. $f: M \to N$ linear map, ker(f) submodule of M and Im(f) submodule of N.

Exercise 1.4. $f: M \to N$ linear is injective $\Leftrightarrow ker(f) = \{0\}$

- **Definition 1.5.** 1. Let S be a subset of M. S is free if $\forall x_1, ..., x_n \in S$, $\forall a_1, ..., a_n \in A$, $a_1x_1 + ..., a_nx_n = 0 \implies a_1 = ... = a_n = 0$;
 - 2. A basis of M is a free subset which generates M;
 - 3. $(M_i)_{i \in I}$ family of A-modules

$$\bigoplus_{i \in I} M_i = \{(a_i)_{i \in I}, a_i = 0, \forall i \in I \text{ except for finitely many of them}\} \subset \prod_{i \in I} M_i$$

If $M_i = A \ \forall i \in I$ then we denote $\bigoplus_{i \in I} M_i = A^{(I)}$.

4. M is a free module if there is a basis (\Leftrightarrow there is an isomorphism $A^{(I)} \equiv M$ for some set I, $A^{(I)} = \bigoplus_{I} A \neq A^{I}$).

Exercise 1.6. Prove the above equivalence.

5. Let N be a submodule of M. M/N is the quotient as group endowed with a natural structure of module by $a * \bar{x} = \bar{ax}$, $\forall a \in A$, $\forall x \in M$, \bar{x} is the class of x mod N. M/N is a A-module, and the canonical $M \to M/N$ is linear

Example 1.7. 1. $n \ge 1$, $\mathbb{Z}/n\mathbb{Z}$ Z-module is not free $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $n \cdot x = 0$

2. \mathbb{Q} \mathbb{Z} -module is not free. If $r \neq 0$, $n \cdot r = 0 \Rightarrow n = 0$, and if $r_1 = p_1/q_1$, $r_2 = p_2/q_2$; $p_i, q_i \in \mathbb{Z}, q_i \neq 0$.

 $(q_1p_2)r_1 - (q_2p_1)r_2 = 0$

If S is a basis of \mathbb{Q} as \mathbb{Z} -module $\Rightarrow S = \{r_0\}$ but $\mathbb{Q} = r_0\mathbb{Z}, 1/2r_0 \notin r_0\mathbb{Z}$.

Exercise 1.8. If M is finitely generated and has a basis, then the basis is finite.

Exercise 1.9. If a finitely generated \mathbb{Z} -module has two different bases, they are the same size.

Exercise 1.10. (ISOMORPHISM THEOREM) If $f : M \to N$ linear surjective map, prove that M/ker(f) is isomorphic to N as modules.

1.1 Noetherian modules:

- **Definition 1.11.** 1. M is A-module is noetherian if every submodule of M is finitely generated (generated by a finite subset).
 - 2. A is noetherian ring if it is noetherian as an A-module over itself. This is equivalent to saying that the ideals of A are finitely generated.

Exercise 1.12. A noetherian, M A-module then M is noetherian if and only if M is finitely generated.

Example 1.13. 1. Fields are noetherian, \mathbb{Z} is noetherian;

2. Theorem (Hilbert) A is noetherian $\Rightarrow A[X]$ is noetherian.

- 3. k field, $k[X_1, ..., X_n]$ is noetherian.
- 4. If A is noetherian then A/I is noetherian $\forall I$ ideal of A.

Exercise 1.14. Prove the converse of Hilbert's Theorem: If A[X] is noetherian $\Rightarrow A$ is noetherian.

1.2 Localization

Definition 1.15. A is a ring. A multiplicative subset S of A is a set such that:

- *1.* $1 \in S$,
- 2. $\forall s, t \in S, st \in S$,

Definition 1.16. $S^{-1}A$ is the localization of A with respect to S. It is defined as the set of equivalence classes $\{a/s, a \in A, s \in S\}$, where equivalence is defined below

 $a/s = b/t \Leftrightarrow (at - bs)s' = 0$, for some $s' \in S$; a/s + b/t = (at + bs)/(st). $a/s \cdot b/t = (ab)/(st)$.

Example 1.17. 1. $a/s = a'/s' \Rightarrow (as' - a's)s'' = 0;$ 2. (at + bs)/(st) = (a't + bs')/(s't)

 $((at+bs)s't - (a't+bs')st = as't^2 + bss't - a'st^2 - bss't = (as-a's)t^2$ is killed by s''

We can check that this defines a structure of commutative unitary ring on $S^{-1}A$, the map $A \to S^{-1}A$ sending a to a/1 is a ring homomorphism.

Remarque 1.18. if A is an integral domain, $S = A - \{0\}$ is multiplicative subset of A. $S^{-1}A$ is a field of fraction of A. If A integral, then $\forall T$ multiplicative subset of A, $T^{-1}A \subset Frac(A)$.

Example 1.19. $A = \mathbb{Q}[X, Y]/(XY) = \mathbb{Q}[x, y], S = \{x^n | n \ge 1\} \cup \{1\} \text{ and } S^{-1}A = \mathbb{Q}[x, 1/x] = \{P(x)/x^n | P(x) \in \mathbb{Q}[x], n \ge 0\}.$

Example 1.20. *1.* Let $f \in A$, $A_f := S^{-1}A$, $S = \{f^n | n \ge 1\} \cup \{1\}$;

2. If f is nilpotent $\Rightarrow 0 \in S$, $\Rightarrow 0 \in S^{-1}A$ is invertible in $S^{-1}A \Rightarrow S^{-1}A = \{0\}$;

3. Let \mathfrak{p} be a prime ideal of A, $A_{\mathfrak{p}} = S^{-1}A$, $S = A - \mathfrak{p}$ multiplicative and δ defined as

of A. We have the following universal property: Let $f : A \to B$ be a ring homomorphism then f factorizes though $S^{-1}A$ if and only if $f(S) \subset B^{\times}$ (invertible)



 \tilde{f} is a ring homomorphism $\tilde{f}(a/s) = f(a)f(s)^{-1}, f(s) \in B$.

Exercise 1.21. Prove the above universal property.

Notation: *B* ring, $Spec(B) = \{ prime \ ideals \ of \ B \}$ (Spectrum of *B*). If $f : A \to B$ ring homomorphism \Rightarrow

$$\begin{array}{rcl} Spec(f): & Spec(B) & \to & Spec(A) \\ & Q & \mapsto & f^{-1}(Q) \end{array}$$

Proposition 1.22. $Spec(f) : Spec(S^{-1}A) \to Spec(A)$ induces a bijection from $Spec(S^{-1}A)$ to $\{Q \in Spec(A) | Q \cap S = \emptyset\}$

Proof. Exercise

M A-module, *S* multi subset of $A \to S^{-1}A$. Let's define $S^{-1}M = \{x/s | x \in M, s \in S\}$

- 1. $x/s = y/t \Leftrightarrow s'(tx sy) = 0$, for some $s' \in S$;
- 2. x/s + y/t = (tx + sy)/(st);
- 3. $a/s \cdot x/t = (ax)/(st)$.

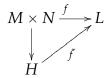
Exercise 1.23. Prove the above definitions are well defined and do make $S^{-1}M$ into a $S^{-1}A$ -module.

Exercise 1.24. Let S be a multiplicatively closed subset of a ring A and let M be a finitely generated A-module. Prove that $S^{-1}M = 0$ if and only if there exists $s \in S$ such that $sM = \{0\}$.

1.3 Tensor product

A ring; M, N A-modules;

Definition 1.25. The tensor product of M, N over A. Let H be a A-module endowed with a bilinear map $\delta : M \times N \to H$ with the universal property for every bilinear map, $f : M \times N \to L$ there exists a unique factorization



with \tilde{f} linear map .

Proposition 1.26. The tensor exists and is unique.

Proof. 1. Uniqueness: Exercise.

2. Existence:

$$A^{(M \times N)}(x, y) \in M \times N,$$

 $e_{(x,y)} = \begin{cases} 1 & \text{in } (x, y) \text{ (coordinate)} \\ 0 & elsewhere \end{cases} \in A^{(M \times N)}$

 $\{e_{(x,y)}|(x,y) \in M \times N\}$ is a basis of $A^{(M \times N)}$. L = submodule of $A^{(M \times N)}$ generally by the element

$$e_{(x_1,x_2,y)} - e_{(x_1,y)} - e_{(x_2,y)}$$
$$e_{(x,y_1+y_2)} - e_{(x,y_1)} - e_{(x,y_2)}$$

 $x_i \in M, y_i \in N.$

$$e_{(ax,y)} - e_{(x,ay)}, e_{(ax,y)} - ae_{(x,y)}, a \in A$$

Prove that $\rho: M \times N \to A^{M \times N}/L$ is a tensor product of M, N over A.

For $x \in M$, $y \in N$, we note $x \otimes y = \rho(x, y)$.

Remarque 1.27. — every of $M \otimes_A N$ can be written as $\sum_{i \text{ finite}} x_i \otimes y_i, x_i \in M$, $y_i \in N$;

 $-x \otimes y = x' \otimes y'$ does not imply a relation between x and x', y and y'.

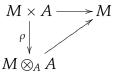
Example 1.28.

$$\mathbb{Z}/2\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/3\mathbb{Z}=\{0\}$$

 $x \otimes y = (3x-2x) \otimes y = 3x \otimes y - 2x/6 \otimes y = x \otimes 3y - 0 \otimes y = x \otimes 0 - 0 \otimes y = f(x,0) - f(0,y) = 0 - 0 = 0$ Exercise 1.29. Show that $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \{0\}$ if m,n are coprime.

Proposition 1.30. A ring, M, N A-modules

- 1. $M \otimes_A A \simeq M$;
- 2. $M \otimes N \simeq N \otimes_A M;$
- 3. $(\bigoplus_i M_i) \otimes_A N \simeq \bigoplus_i (M_i \otimes_A N);$
- 4. $L \otimes (M \otimes N) \simeq (L \otimes M) \otimes N$.
- *Proof.* 1. $M \otimes_A A \simeq M$ sending $x \otimes a = (ax) \otimes 1$ to ax. Let $M \times A \to M$ sending (x, a) to xa. It is a bilinear map such that the following diagram is commutative:



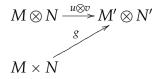
- 2. same kind of proof: we define $M \otimes_A N \simeq N \otimes_A M$ by mapping $x \otimes y$ to $y \otimes x$.
- 3. We define $(\bigoplus_i M_i \otimes_A N \simeq \bigoplus_i (M_i \otimes_A N)$ by mapping $(x_i)_i \otimes y \mapsto (x_i \otimes y)_i$.

Corollary 1.31. If M is free over A with a basis $(e_{\alpha})_{\alpha}$ then every elements $g \ M \otimes_A N$ can be written uniquely as $\sum_{\alpha} e_{\alpha} \otimes y_{\alpha}, y_{\alpha} \in N$,

$$\begin{array}{rcl} (\oplus_i M_i) \otimes_A N &\simeq & \oplus_i (M_i \otimes_A N) \\ (x_i)_i \oplus y & \mapsto & (x_i \otimes y)_i \end{array}$$

Proof. use Proposition (c)

Tensor products of linear maps M,N,M',N' A-modules $u:M\to N',\,v:M'\to N'$



where g sends (x, y) to $u(x) \otimes v(x)$ is bilinear and $(u \otimes v)(x \oplus y) = u(x) \otimes v(y)$.

1.4 Base change or extension of scalars:

A ring, $\pi : A \to B$ ring homomorphism. If N is a B-module then N is a A-module. $a \in A, x \in N, x * a = \pi(a)x$. If M is a A-module, $B \otimes_A M$ is a B-module, $b * (\sum_i b_i \otimes x_i) = \sum_i (bb_i) \otimes x_i \ b_i \in B, x_i \in M, b \in B$. Fix $b \in B$, we define the morphism $b : B \otimes M \to B \otimes M \to B \otimes M$ sending (c, x) to $(bc) \otimes x$

2 Complex of modules over A

Definition 2.1.

$$\longrightarrow M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \dots \ (*)$$

 M_i A-module f_i linear maps.

- 1. (*) is a complex if $f_{i+1} \circ f_i = 0$ $\forall i$, that is $Im(f_i) \subset ker(f_{i+1})$.
- 2. A complex (*) is exact if $Im(f_i) = ker(f_{i+1}) \forall i$ (exact sequence).

Example 2.2. The complex

$$0 \longrightarrow M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \longrightarrow 0$$

- 1. is exact at right if f_1 is surjective;
- 2. is exact at left if f_0 is injective;
- 3. is exact at the middle if $Im(f_0) = Ker(f_1)$.

Exercise 2.3. Let $0 \longrightarrow M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \longrightarrow 0$ be an exact sequence of A-modules. If M_0 , M_2 are finitely generated, so is M.

Proposition 2.4. Let

$$0 \longrightarrow M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \longrightarrow 0$$

be a short exact sequence. Let N be a A-module then, the complex

$$0 \longrightarrow M_0 \otimes_A N \xrightarrow{f_0} M_1 \otimes_A N \xrightarrow{f_1} M_2 \otimes_A N \longrightarrow 0$$

is exact (at right), that is $M_1 \otimes_A N \twoheadrightarrow M_2 \otimes_A N$.

Proof. Exercise.

Corollary 2.5. I ideal of A, M A-module then $M \otimes_A A/I \simeq M/IM$

Proof. Exercise

Remarque 2.6. $I \otimes_A M \twoheadrightarrow IM$ (surjective but in general not injective.)

Example 2.7. $A = \mathbb{Z}, M = \mathbb{Z}/2\mathbb{Z}, I = 2\mathbb{Z}, IM = 2M = 0.$ $I \simeq A, I \otimes_A M \simeq A \otimes_A M \simeq M \neq 0.$

Definition 2.8. We say that M is a flat A-module if $\forall I$ ideal of A, the canonical map $I \otimes_A M \to IM$ is an isomorphism ($\Leftrightarrow I \otimes_A M \to M$ injective, sending $\alpha \mapsto \alpha x$.)

Theorem 2.9. *M* is flat \Leftrightarrow for any injective morphism $N_1 \rightarrow N_2$ linear map of *A*-module then *M* is flat \Leftrightarrow *M* is torsion free.

Let M be a module on an integral domain A. M is torsion free, if ax = 0, $a \in A$ $\Rightarrow a = 0$ or x = 0 that is equivalent to $\forall a \in A \setminus \{0\}$, $\cdot a : M \to M$ sending x to ax is injective.

Proof. Exercise.

Exercise 2.10. 1. Let A be a nonzero ring. Show that $A^m \simeq A^n$ then m = n.

- 2. Could you use the same proof to show that if $f : A^m \to A^n$ is surjective, then $m \ge n$?
- 3. Could you use the same proof to show that if $f : A^m \to A^n$ is injective, then $m \leq n$?

2.1 Tensor product of algebras

Definition 2.11. A is a ring, a A-algebra is a (commutative unitary) ring B endowed with a ring homomorphism $A \rightarrow B$.

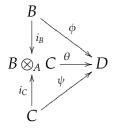
Example 2.12. *1.* $A[X_1, ..., X_n]$ *is a A-algebra.*

- 2. $A[X_1, ..., X_n]/I$ is a A-algebra/
- 3. Any ring is uniquely a \mathbb{Z} -algebra ($\forall B \text{ ring } \exists ! \text{ ring homomorphism } \mathbb{Z} \to B \text{ sending } k \text{ to } k \cdot 1_B.$

Definition 2.13. A finite generated A algebra is a A-algebra isomorphic to $A[x_1, ..., x_n]/I$

B, C A-algebra, $B \otimes_A C$ exists as A-module and has a structure of A-algebra. We define the product as $(\sum b_i \otimes c_i)(\sum b'_j \otimes c'_j) = \sum b_i b'_j \otimes c_i c'_j$. It is well defined (independent of the representative) $A \to B \otimes_A C$ sending a to $a \otimes 1 = 1 \otimes a$ ring homomorphism.

Proposition 2.14. Given B, C two algebra. For any A-algebra D, and ring homomorphism $\phi: B \to D, \psi: C \to D$, there exists a unique ring homomorphism $B \otimes_A C \to D$.



is commutative. Here, i_B sends b to $b \otimes 1$ and c to $1 \otimes c$.

Proof. Exercise.

2.2 Nakayama lemma

Theorem 2.15. (a, \mathfrak{m}_0) a local ring (i.e. \mathfrak{m} the unique maximal ideal of A. Let M be a finitely generated A-module such that $M = \mathfrak{m}_0 M$ then M = 0.

Proof. Exercise.

Proposition 2.16. Let M be a A-module then M is flat if and only if for any B prime ideal of A, $M \otimes_A B$ is flat over B if and only if for any \mathfrak{m} maximal ideal of A, $M \otimes_A A_{\mathfrak{m}}$ is flat over $A_{\mathfrak{m}}$

Proof. Exercise.

Exercise 2.17. Prove that if A is a local ring, M and N are finitely generated A-modules, and $M \otimes_A N = 0$, then one of M or N is zero.

Theorem 2.18. Let (A, \mathfrak{m}) be a local ring. Let M be a finitely generated A-module then M is flat if and only if M is free.

Proof. M free $\Rightarrow M$ flat in general even if M is not finitely generated. Suppose that M is flat $M \otimes_A A/\mathfrak{m} = M \otimes_A j \simeq M/\mathfrak{m} M \rightarrow k = A/\mathfrak{m}$ (k is a field the residue field of A.) is a vector space over k of finite dimension. If $x_1, ..., x_n \in M$ are such that $\bar{x_1}, ..., \bar{x_n} \in M \otimes_A k$ is a basis.

We want to prove $\{x_1, ..., x_n\}$ is a bases of M over A.

- 1. If $\{x_1, ..., x_n\}$ in M such that $\{\bar{x_1}, ..., \bar{x_n}\}$ genrates $M \otimes k$ implies $\{x_1, ..., x_n\}$ generates M.
- 2. If $\{x_1, ..., x_n\}$ in M such that $\{\overline{x_1}, ..., \overline{x_n}\}$ is free implies $\{x_1, ..., x_n\}$ is free.

LEFT IN EXERCISE

Exercise 2.19. If M and N are flat A-modules, then so is $M \otimes_A N$.

8

3 Hilbert Nullstellensatz

Theorem 3.1. (Hilbert Nullstellensatz) $A \to B$, $B \ a \ A$ -algebra, $b \in B$ is integral over A if there is $a_0, ..., a_{n-1} \in A$ such that $a_0 + a_1b + \cdots + a_{n-1}b^{n-1} + b^n = 0$:

- 1. $\{b \in B, b \text{ integral over } A\}$ subring of A;
- 2. B is finitely over A (definition is finitely generated as A-module) \Leftrightarrow B is integral over A and finitely generated as A-algebra.

k field

Lemma 3.2. (Noether normalization lemma) If B is a finitely generated k-algebra then there exists a finite ring homomorphism $k[X_1, ..., X_n] \hookrightarrow B$.

Theorem 3.3. (Weak Hilbert Nullstellensatz) Let \mathfrak{m} be a maximal ideal of $k[X_1, ..., X_n]$ then $k \to k[X_1, ..., X_n]/\mathfrak{m}$ is a finite extension (if $k = \overline{f}$ algebraically closed, then $k[X_1, ..., X_n]/\mathfrak{m} \simeq k$ and $\mathfrak{m} = (X_1 - \alpha_1, ..., X_n - \alpha_n)$.

Theorem 3.4. (Strong Nullstellensatz) For any ideal of $k[X_1, ..., X_n]$,

$$\sqrt{I} = \bigcap_{\mathfrak{m} \text{ maximal ideal containing } I} \mathfrak{m}$$

Corollary 3.5. Suppose that $k = \overline{k}$, let I be an ideal of $k[X_1, ..., X_n]$, let

$$Z(I) = \{(\alpha_1, ..., \alpha_n) \in k^n | P(\alpha_1, ..., \alpha_n) = 0, \forall P \in I\}$$

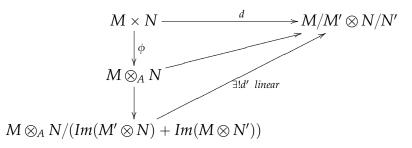
Let $F \in k[X_1, ..., X_n]$ then $F(x) = 0, \forall x \in Z(I) \Leftrightarrow F \in \sqrt{I}$.

M, N A-modules $M' \subseteq M, N' \subseteq N$,

$$M/M' \otimes_A N/N' \simeq M \otimes_A N/(Im(M' \otimes N) + Im(M \otimes N'))$$

$$i: M' \to m, \ i_N = i \otimes Id_n: M' \otimes_A N \to M \otimes_A N$$

 $b: M/N' \times N/N' \to M \otimes_A N/(Im(M' \otimes N) + Im(M \otimes N')) \text{ bilinear sending } (\bar{x}, \bar{y}) \text{ to } \overline{x \otimes y}$ $\Rightarrow b: M/N' \otimes_A N/N' \to M \otimes_A N/(Im(M' \otimes N) + Im(M \otimes N')) \text{ sending } \bar{x} \otimes \bar{y} \text{ to } \overline{x \otimes y}$ Let $d: M \times N \to M/M' \otimes N/N'$ bilinear sending (x, y) to $\bar{x} \otimes \bar{y}$



 $Im(M' \otimes N) + Im(M \otimes N') \subset ker(\tilde{d}), d'(x' \otimes y + x \otimes y') = \bar{x}' \otimes \bar{y} + \bar{x} \otimes \bar{y}' = 0.$ We check that \tilde{b} and \tilde{d} are inverse one from another.

Exercise 3.6. Explain how to deduce the Weak Nullstellensatz from the Strong Nullstellensatz.