Math200b, homework 3

Golsefidy

January 2019

Localizing a module.

Reading before problem. Suppose A is a unital commutative ring, $S \subseteq A$ is a multiplicatively closed subset, and M is an A-module. We can localize M with respect to S as we did A. Namely on $M \times S$ we define the following relation:

$$(m_1, s_1) \sim (m_2, s_2) \Rightarrow \exists s \in S, s(s_1 m_2 - s_2 m_1) = 0.$$

Convince yourself that $\sim$ is an equivalence relation on $M \times S$, and let $\frac{m}{s} := [(m, s)]$, and

$$S^{-1}M := \{\frac{m}{s} | \, m \in M, s \in S\}.$$

Let $\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$; convince yourself that this is a well-defined operation and $(S^{-1}M, +)$ is an abelian group.

For $\frac{a}{s} \in S^{-1}A$ and $\frac{m}{s'} \in S^{-1}M$, let $\frac{a}{s} \cdot \frac{m}{s'} := \frac{am}{ss'}$. Convince yourself that it is well-defined, and it makes $S^{-1}M$ an $S^{-1}A$-module.

For $\mathfrak{p} \in \mathrm{Spec}(A)$, we let $M_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1}M$ where $S_{\mathfrak{p}} := A \setminus \mathfrak{p}$.

1. Suppose M is an A-module. Prove that

$$\begin{aligned} M = 0 &\iff \forall \mathfrak{p} \in \mathrm{Spec}(A), M_{\mathfrak{p}} = 0 \\ &\iff \forall \mathfrak{m} \in \mathrm{Max}(A), M_{\mathfrak{m}} = 0. \end{aligned}$$

   (**Hint**: Clearly the only non-trivial part is why $\forall \mathfrak{m} \in \mathrm{Max}(A), M_{\mathfrak{m}} = 0$ implies $M = 0$. For $x \in M$, consider $\mathrm{ann}(x) := \{a \in A | ax = 0\}$ and show that it cannot be proper.)

2. Let $\phi : M_1 \to M_2$ be an A-module homomorphism. Suppose S is a multiplicatively closed subset of A. Let $S^{-1}\phi : S^{-1}M_1 \to S^{-1}M_2, (S^{-1}\phi)(\frac{m_1}{s}) := \frac{\phi(m_1)}{s}$. Show that $S^{-1}\phi$ is a well-defined $S^{-1}A$-module homomorphism.

   (For $\mathfrak{p} \in \mathrm{Spec}(A)$, we let $\phi_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1}\phi$ where $S_{\mathfrak{p}} := A \setminus \mathfrak{p}$.)

(Note: suppose M_1 is a submodule of M_2. Observe that $S^{-1}M_1$ is a submodule of $S^{-1}M_2$ and convince yourself that $S^{-1}M_2/S^{-1}M_1 \simeq S^{-1}(M_2/M_1)$.)

3. Let $\phi : M_1 \to M_2$ be an A-module homomorphism. Prove that

$$\phi \text{ is injective} \iff \forall \mathfrak{m} \in \operatorname{Max}(A), \phi_{\mathfrak{m}} \text{ is injective.}$$

(**Hint**: Show that $\ker \phi_{\mathfrak{m}} = (\ker \phi)_{\mathfrak{m}}$.)

4. Show that

$$\phi \text{ is surjective} \iff \forall \mathfrak{m} \in \operatorname{Max}(A), \phi_{\mathfrak{m}} \text{ is surjective.}$$

(**Hint**: Consider the co-kernel of ϕ; that means $M_2/\operatorname{Im}\phi$. And the co-kernels of $\phi_{\mathfrak{m}}$.)

Spec of a localized ring.

Reading before problem. Suppose A is a unital commutative ring and S is a multiplicatively closed set. As we saw above, if $\mathfrak{a} \trianglelefteq A$, then $S^{-1}\mathfrak{a} \trianglelefteq S^{-1}A$; and $S^{-1}(A/\mathfrak{a}) \simeq S^{-1}A/S^{-1}\mathfrak{a}$ as

$S^{-1}A$-modules. Convince yourself that this implies $\overline{S}^{-1}(A/\mathfrak{a}) \simeq S^{-1}A/S^{-1}\mathfrak{a}$ as rings where $\overline{S} := \{s + \mathfrak{a} \in A/\mathfrak{a} \mid s \in S\}$.

1. Suppose $\widetilde{\mathfrak{a}}$ is an ideal of $S^{-1}A$. Let

$$\mathfrak{a} := \{a \in A \mid \frac{a}{1} \in \widetilde{\mathfrak{a}}\}.$$

Prove that $\mathfrak{a} \trianglelefteq A$ and $\widetilde{\mathfrak{a}} = S^{-1}\mathfrak{a}$.

2. Let $\mathcal{O}_S := \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \varnothing\}$. Let

$$\Phi : \mathcal{O}_S \longrightarrow \operatorname{Spec}(S^{-1}A),\, \Phi(\mathfrak{p}) := S^{-1}\mathfrak{p},$$

and

$$\Psi : \operatorname{Spec}(S^{-1}A) \longrightarrow \mathcal{O}_S,\, \Psi(\widetilde{\mathfrak{p}}) := \{a \in A \mid \frac{a}{1} \in \widetilde{\mathfrak{p}}\}.$$

Prove that Φ and Ψ are well-defined and they are inverse of each other.

(And so there is a bijection between prime ideals of $S^{-1}A$ and prime ideals of A that do not intersect S.)

(**Hint**: **(a)** You have to show $S^{-1}\mathfrak{p}$ is prime if $\mathfrak{p}$ is prime. **(b)** Think about

$$S^{-1}A/S^{-1}\mathfrak{p} \simeq \overline{S}^{-1}(A/\mathfrak{p}) \hookrightarrow \text{ field of fractions of } A/\mathfrak{p}.$$

(c) Next you have to show

$$\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec} A, S^{-1}\mathfrak{p}_1 = S^{-1}\mathfrak{p}_2 \Rightarrow \mathfrak{p}_1 = \mathfrak{p}_2.)$$

Rank vs minimum number of generators.

Reading before problem. A module M is called Noetherian if the following (equivalent) statements hold:

(a) Any chain $\{N_i\}_{i\in I}$ of submodules of M has a maximal.

(b) Any non-empty set Σ of submodules of M has a maximal element.

(c) M satisfies the ascending chain condition (a.c.c.); that means if $N_1 \subseteq N_2 \subseteq \cdots$ are submodules of M, then $\exists i_0$ such that $N_{i_0} = N_{i_0+1} = \cdots$.

(d) All the submodules of M are finitely generated.

Go over Lecture 18 of math 200a and see that similar arguments imply the above statements are equivalent.

Observe that A is a Noetherian ring if and only if A is a Noetherian A-module.

1. (a) Suppose N is a submodule of M. Prove that

$$M \text{ is Noetherian } \iff N \text{ and } M/N \text{ are Noetherian.}$$

(b) Suppose A is a Noetherian ring, and M is a finitely generated A-module. Prove that M is Noetherian.

2. (a) Suppose A is a Noetherian unital commutative ring, and $\phi : A^n \to A^m$ is an injective A-module homomorphism. Prove that $n \leq m$.

(**Hint**: If not, $\phi(A^n) \oplus A^{n-m} \subseteq A^n$; use this to deduce that for any $i \in \mathbb{Z}^+$ we have

$$\phi^i(A^n) \oplus \phi^{i-1}(A^n - m) \oplus \phi^{i-2}(A^{n-m}) \oplus \cdots \oplus A^{n-m} \subseteq A^n;$$

from here deduce that

$$\begin{aligned} A^{n-m} &\subsetneq A^{n-m} \oplus \phi(A^{n-m}) \\ &\subsetneq A^{n-m} \oplus \phi(A^{n-m}) \oplus \phi^2(A^{n-m}) \subsetneq \cdots \subseteq A^n.) \end{aligned}$$

(b) Suppose A is a unital commutative ring, and $\phi : A^n \to A^m$ is an A-module homomorphism. Prove that $n \le m$.

(**Hint**: Suppose $x_\phi := [a_{ij}]$ is the associated matrix; and let A_0 be the subring of A which is generated by a_{ij}'s. Consider $\phi|_{A_0^n}$, discuss why $\phi|_{A_0^n} : A_0^n \to A_0^m$ is an injective A_0-module homomorphism. Use Hilbert's basis theorem and part (a) to finish the proof.)

(c) Suppose A is a unital commutative ring, and M is a finitely generated A-module. Let

$$d(M) := \text{minimum number of generators of } M,$$
$$\operatorname{rank}(M) := \text{maximum number of } A\text{-linearly independent elements of } M.$$

Prove that $\operatorname{rank}(M) \le d(M)$.

(**Hint**: Let $d(M) = n$ and $\operatorname{rank}(M) = m$. Then there are a surjective A-module homomorphism $\phi : A^n \to M$ and an injective A-module homomorphism $\psi : A^m \to M$. So, for any $1 \le i \le m$, $\exists v_i \in A^n$ such that $\phi(v_i) = \psi(e_i)$ where e_i's are the standard A-basis of A^m. Let $\theta(e_i) := v_i$ and extend it to an A-module hom $\theta : A^m \to A^n$ such that

$\begin{array}{ccc} A^m & & \\ {\scriptstyle\theta}\,\downarrow & \overset{\psi}{\searrow} & \\ A^n & \xrightarrow{\phi} & M \end{array}$ is a commuting diagram. Deduce that θ is injective and finish the proof.)

(Note: In class, we proved the case where A is an integral domain.)

3. Suppose A is a unital commutative ring and M is an A-module. Suppose $d(M) = \mathrm{rank}(M) = n$. Prove that $M \simeq A^n$.

(**Hint**: As above there is θ such that $\begin{array}{ccc} A^n & & \\ {\scriptstyle\theta}\,\downarrow & \overset{\psi}{\searrow} & \\ A^n & \xrightarrow{\phi} & M \end{array}$ is a commuting diagram. Deduce that

$$\theta(A^n) \oplus \ker \phi \subseteq A^n. \tag{1}$$

Based on an argument similar to 2(a) and (1) get a contradiction if A is Noetherian and $\ker \phi \neq 0$. Finish the proof based on a similar argument as in 2(b).)

Smith form and its applications.

1. Let D be a PID and F be its field of fractions. For $A \in M_{n,m}(D)$, let

$$N_A(F) := \{v \in F^m \mid Av = 0\} \text{ and } N_A(D) := N_A(F) \cap D^m$$
$$R_A(F) := \{Av \in F^n \mid v \in F^m\}$$
$$R_A(D) := \{Av \in D^n \mid v \in D^m\}.$$

(a) Prove that $D^m/N_A(D)$ is a free D-module; and deduce that D^m has a D-basis $x_1, \ldots, x_m$ such that $N_A(D) = Dx_{r+1} \oplus \cdots \oplus Dx_m$, where $r = \dim_F R_A(F)$.

(b) Prove that there is a D-basis $y_1, \cdots, y_n$ of D^n and $d_1, \cdots, d_r \in D$ such that

$$d_1 | \cdots | d_r, \text{ and } R_A(D) = Dd_1y_1 \oplus \cdots \oplus Dd_ry_r,$$

where $r = \dim_F R_A(F)$.

(c) Let x_i's be as in part (a). Prove that there is a D-basis $\{x'_1, \cdots, x'_r\}$ of $Dx_1 \oplus \cdots \oplus Dx_r$ such that $Ax'_i = d_iy_i$ for any $1 \le i \le r$.

(d) Prove that

$$[x_1' \cdots x_r' x_{r+1} \cdots x_m] \in \mathrm{GL}_m(D),\ [y_1 \cdots y_n] \in \mathrm{GL}_n(D),$$

and

$$A[x_1' \cdots x_r' x_{r+1} \cdots x_m] = [y_1 \cdots y_n] \begin{pmatrix} \mathrm{diag}(d_1, d_2, \ldots, d_r) & 0 \\ 0 & 0 \end{pmatrix}$$

where $\mathrm{diag}(d_1, d_2, \ldots, d_r)$ is the diagonal matrix with diagonal entries d_i's.

(e) (Smith form of A) Prove that there are $\gamma_1 \in \mathrm{GL}_n(D)$, $\gamma_2 \in \mathrm{GL}_m(D)$ and $d_1 | d_2 | \cdots | d_r$ in D such that

$$A = \gamma_1 \begin{pmatrix} \mathrm{diag}(d_1, d_2, \ldots, d_r) & 0 \\ 0 & 0 \end{pmatrix} \gamma_2.$$

2. Let $A \in M_n(\mathbb{Z})$, and $M_A := \mathbb{Z}^n / R_A(\mathbb{Z})$. Suppose $A = \gamma_1 \begin{pmatrix} \mathrm{diag}(d_1, d_2, \ldots, d_m) & 0 \\ 0 & 0 \end{pmatrix} \gamma_2$ is a Smith form of A.

(a) Prove that $M_A \simeq \mathbb{Z}^{n-m} \oplus \bigoplus_{i=1}^{m} \mathbb{Z}/d_i\mathbb{Z}$.

(b) Prove that M_A is finite if and only if $\det A \neq 0$.

(c) Suppose $\det A \neq 0$. Prove that $|M_A| = |\det A|$.

3. Let k be a field, and $A \in M_n(k[x])$. Suppose $\det A \neq 0$. Suppose $A = \gamma_1 \begin{pmatrix} \mathrm{diag}(d_1(x), d_2(x), \ldots, d_m(x)) & 0 \\ 0 & 0 \end{pmatrix} \gamma_2$ is a Smith form of A.

   (a) Prove that $m = n$ and (as $k[x]$-modules)

$$k[x]^n / R_A(k[x]) \simeq \bigoplus_{i=1}^{n} k[x]/d_i(x)k[x].$$

   (b) Prove that $\dim_k (k[x]^n / R_A(k[x])) = \deg(\det(A))$.

4. Let k be a field, and $A \in M_n(k)$. Suppose

$$xI - A = \gamma_1 \begin{pmatrix} \mathrm{diag}(f_1(x), f_2(x), \ldots, f_m(x)) & 0 \\ 0 & 0 \end{pmatrix} \gamma_2$$

   is a Smith form of $xI - A \in M_n(k[x])$. Suppose m is the largest integer such that $\deg f_{m-1} = 0$.

   (a) Think about k^n as a $k[x]$-module with scalar multiplication $x \cdot v := Av$. Let

$$\phi : k[x]^n \to k^n, \phi\left(\sum_{i=0}^{\infty} x^i v_i\right) := \sum_{i=0}^{\infty} A^i v_i$$

   for $v_i \in k^n$. Prove that ϕ is a $k[x]$-module homomorphism and $\ker \phi = R_A(k[x])$.

(b) Prove that as $k[x]$-modules

$$k[x]^n / R_A(k[x]) \simeq \bigoplus_{i=m}^{n} k[x]/f_i(x)k[x].$$

(c) Prove that $\mathrm{diag}(c(f_m), \ldots, c(f_n))$ is the rational canonical form of A where $c(f_i)$ is the companion matrix of the polynomial f_i.

(Note: This gives us an effective algorithm to find invariant factors of a matrix.)