MATH200C, LECTURE 7

GOLSEFIDY

Localization

We were proving the following:

Lemma 1. *Let $f : A \to S^{-1}A, f(a) := a/1$. Then f^* induces a bijection between* $\mathrm{Spec}(S^{-1}A)$ *and* $\{\mathfrak{p} \in \mathrm{Spec}(A) | \, \mathfrak{p} \cap S = \varnothing\}$. *Moreover if* $\mathfrak{p} \in \mathrm{Spec}(A)$ *and* $\mathfrak{p} \cap S = \varnothing$, *then* $\mathfrak{p}^{ec} = \mathfrak{p}$.

Proof. (Continue) We have already proved that f^* is injective and $f^*(\widetilde{\mathfrak{p}}) \cap S = \varnothing$. We were in the middle of the third step.

Step 3. Suppose $\mathfrak{p} \in \mathrm{Spec}(A)$ and $\mathfrak{p} \cap S = \varnothing$. Then $A/\mathfrak{p}$ is an integral domain and $\overline{S} := \pi(S)$ does not contain 0, where $\pi : A \to A/\mathfrak{p}, \pi(a) := a + \mathfrak{p}$. Hence $\overline{S}^{-1}(A/\mathfrak{p})$ can be embedded into the field $Q(A/\mathfrak{p})$ of fractions of $A/\mathfrak{p}$. Let θ be the composite $A \to A/\mathfrak{p} \hookrightarrow Q(A/\mathfrak{p})$ homomorphism. Then $\theta(S) \subseteq Q(A/\mathfrak{p})^\times$; hence by the universal property of localization, there is a ring homomorphism $\widetilde{\theta} : S^{-1}A \to Q(A/\mathfrak{p}), \widetilde{\theta}(a/s) := \pi(a)/\pi(s)$. Notice that

$$a/s \in \ker \widetilde{\theta} \Leftrightarrow \pi(a)/\pi(s) = 0 \Leftrightarrow \pi(a) = 0 \Leftrightarrow a \in \mathfrak{p}.$$

Therefore $\ker \widetilde{\theta} = S^{-1}\mathfrak{p}$, which implies that $S^{-1}A/S^{-1}\mathfrak{p}$ can be embedded into $Q(A/\mathfrak{p})$; and so it is either an integral domain or it is zero. Thus either $S^{-1}\mathfrak{p} \in \mathrm{Spec}(S^{-1}A)$ or $S^{-1}\mathfrak{p} = S^{-1}A$.

Step 4. Suppose $\mathfrak{p} \in \mathrm{Spec}(A)$ and $\mathfrak{p} \cap S = \varnothing$. We know that $\mathfrak{p}^{ec} \supseteq \mathfrak{p}$. If $x \in \mathfrak{p}^{ec}$, then $x/1 \in S^{-1}\mathfrak{p}$. Hence there is $s \in S$ such that $sx \in \mathfrak{p}$. As $\mathfrak{p}$ is prime, either $s \in \mathfrak{p}$ or $x \in \mathfrak{p}$. Since $\mathfrak{p} \cap S = \varnothing$, we deduce that $x \in \mathfrak{p}$. Thus $\mathfrak{p}^{ec} = \mathfrak{p}$. □

Fiber over a prime ideal

Theorem 2. *Suppose $f : A \to B$ is a ring homomorphism and* $\mathfrak{p} \in \mathrm{Spec}(A)$. *Let* $S_\mathfrak{p} := A \setminus \mathfrak{p}$, *and θ be the composite the following homomorphisms*

$$B \xrightarrow{i} f(S_\mathfrak{p})^{-1}B \xrightarrow{\pi} f(S_\mathfrak{p})^{-1}B/f(S_\mathfrak{p})^{-1}\mathfrak{p}^e.$$

Then

1. θ^* *gives us a bijection between* $\operatorname{Spec}(f(S_{\mathfrak{p}})^{-1}B/f(S_{\mathfrak{p}})^{-1}\mathfrak{p}^e)$ *and* $(f^*)^{-1}(\mathfrak{p})$*.*
2. $B\otimes_A Q(A/\mathfrak{p})\simeq f(S_{\mathfrak{p}})^{-1}B/f(S_{\mathfrak{p}})^{-1}\mathfrak{p}^e$*; and so there is a bijection between* $\operatorname{Spec}(B\otimes_A Q(A/\mathfrak{p}))$ *and* $(f^*)^{-1}(\mathfrak{p})$*.*
3. $\mathfrak{p}\in\operatorname{Im}(f^*)$ *if and only if* $\mathfrak{p}^{ec}=\mathfrak{p}$*.*

Proof. (1) Notice that $\theta^*=i^*\circ\pi^*$. We have proved that i^* induces a bijection between $\operatorname{Spec}(f(S_{\mathfrak{p}})^{-1}B)$ and

$$\{\mathfrak{q}\in\operatorname{Spec}B|\ \mathfrak{q}\cap f(S_{\mathfrak{p}})=\varnothing\}=\{\mathfrak{q}\in\operatorname{Spec}B|\ f^*(\mathfrak{q})\subseteq\mathfrak{p}\};$$

and π^* induces a bijection between $\operatorname{Spec}(f(S_{\mathfrak{p}})^{-1}B/f(S_{\mathfrak{p}})^{-1}\mathfrak{p}^e)$ and

$$V(f(S_{\mathfrak{p}})^{-1}\mathfrak{p}^e)=\{\widetilde{\mathfrak{q}}\in\operatorname{Spec}(f(S_{\mathfrak{p}})^{-1}B)|\ f(S_{\mathfrak{p}})^{-1}\mathfrak{p}^e\subseteq\widetilde{\mathfrak{q}}\}.$$

We have

$$\begin{aligned}\widetilde{\mathfrak{q}}\in V(f(S_{\mathfrak{p}})^{-1}\mathfrak{p}^e)&\Leftrightarrow\exists!\mathfrak{q}\in\operatorname{Spec}B, f^*(\mathfrak{q})\subseteq\mathfrak{p},\widetilde{\mathfrak{q}}=f(S_{\mathfrak{p}})^{-1}\mathfrak{q}, f(S_{\mathfrak{p}})^{-1}\mathfrak{p}^e\subseteq f(S_{\mathfrak{p}})^{-1}\mathfrak{q}\\&\Leftrightarrow\exists!\mathfrak{q}\in\operatorname{Spec}B,\widetilde{\mathfrak{q}}=f(S_{\mathfrak{p}})^{-1}\mathfrak{q}, f^*(\mathfrak{q})\subseteq\mathfrak{p},\mathfrak{p}^e\subseteq\mathfrak{q}\\&\Leftrightarrow\exists!\mathfrak{q}\in\operatorname{Spec}B,\widetilde{\mathfrak{q}}=f(S_{\mathfrak{p}})^{-1}\mathfrak{q}, f^*(\mathfrak{q})\subseteq\mathfrak{p},\mathfrak{p}\subseteq f^*(\mathfrak{q})\\&\Leftrightarrow\exists!\mathfrak{q}\in\operatorname{Spec}B,\widetilde{\mathfrak{q}}=f(S_{\mathfrak{p}})^{-1}\mathfrak{q}, f^*(\mathfrak{q})=\mathfrak{p}.\end{aligned}$$

(Notice that $\mathfrak{p}^e\subseteq\mathfrak{q}$ implies $\mathfrak{p}^{ec}\subseteq\mathfrak{q}^c$; and so $\mathfrak{p}\subseteq\mathfrak{q}^c$. And $\mathfrak{p}\subseteq\mathfrak{q}^c$ implies $\mathfrak{p}^e\subseteq\mathfrak{q}^{ce}\subseteq\mathfrak{q}$. Hence $\mathfrak{p}^e\subseteq\mathfrak{q}\Leftrightarrow\mathfrak{p}\subseteq\mathfrak{q}^c$.) Overall we get the claim.

Part (2) is part of your HW assignment.

(3)

$$\begin{aligned}\mathfrak{p}\in\operatorname{Im}(f^*)\Leftrightarrow&(f^*)^{-1}(\mathfrak{p})\neq\varnothing\\\Leftrightarrow&f(S_{\mathfrak{p}})^{-1}\mathfrak{p}^e\neq f(S_{\mathfrak{p}})^{-1}B\\\Leftrightarrow&\mathfrak{p}^e\cap f(S_{\mathfrak{p}})=\varnothing\Leftrightarrow\mathfrak{p}^{ec}\cap S_{\mathfrak{p}}=\varnothing\\\Leftrightarrow&\mathfrak{p}^{ec}\subseteq\mathfrak{p}\Leftrightarrow\mathfrak{p}^{ec}=\mathfrak{p}.\end{aligned}$$

□

Nakayama's lemma

In math200B you have learned about Nakayama's lemma. Now we give an alternative approach which shows a more general result.

Proposition 3. *Suppose M is a finitely generated A-module, $\phi \in \mathrm{End}_A(M)$, $\mathfrak{a} \trianglelefteq A$, and $\phi(M) \subseteq \mathfrak{a}M$. Then*

$$\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_1\phi + a_0 = 0 \tag{1}$$

for some $a_i \in \mathfrak{a}$.

Proof. Let $\widetilde{R} := \mathrm{End}_A(M)$. We know that $\widetilde{R}$ is a ring (which is not necessarily commutative). We have also seen that $A \to \widetilde{R}, a \mapsto \overline{a}$, where $\overline{a}(m) := a \cdot m$ is a ring homomorphism. Let $\overline{A} := \{\overline{a} | \; a \in A\}$. Then $R := \overline{A}[\phi]$ is a commutative subring of $\widetilde{R}$. If carefully written, (1) is an equation in R:

$$\phi^n + \overline{a}_{n-1}\phi^{n-1} + \cdots + \overline{a}_1\phi + \overline{a}_0 = 0.$$

Suppose $M = Am_1 + \cdots + Am_k$. Then an element $\psi \in \widetilde{R}$ is zero if and only if $\psi(m_i) = 0$ for any i; and so it is enough to show for some a_j's,

$$(\phi^n + \overline{a}_{n-1}\phi^{n-1} + \cdots + \overline{a}_1\phi + \overline{a}_0)(m_i) = 0$$

for any i.

Since $\phi(M) \subseteq \mathfrak{a}M$, for any i, there are $a_{ij} \in \mathfrak{a}$ such that

$$\phi(m_i) = a_{i1}m_1 + \cdots + a_{ik}m_k.$$

Symbolically these equations can be written as

$$\underbrace{\begin{pmatrix} \overline{a}_{11} & \cdots & \overline{a}_{1k} \\ \vdots & \ddots & \vdots \\ \overline{a}_{k1} & \cdots & \overline{a}_{kk} \end{pmatrix}}_{T} \underbrace{\begin{pmatrix} m_1 \\ \vdots \\ m_k \end{pmatrix}}_{\vec{m}} = \begin{pmatrix} \phi(m_1) \\ \vdots \\ \phi(m_k) \end{pmatrix}.$$

Hence $(\phi I - T)\vec{m} = 0$; multiplying both sides by the adjoint of $\phi I - T$ in $M_k(R)$, we get

$$\det(\phi I - T)\vec{m} = 0.$$

This means $\det(\phi I - T) = 0$. Notice that $xI - T = xI \pmod{\mathfrak{a}}$; and so $\det(xI - T) = x^k \pmod{\mathfrak{a}}$. That means there are $a_i \in \mathfrak{a}$ such that

$$\det(xI - T) = x^k + \overline{a}_{k-1}x^{k-1} + \cdots + \overline{a}_0.$$

Therefore

$$\phi^k + \overline{a}_{k-1}\phi^{k-1} + \cdots + \overline{a}_0 = 0.$$

□

Corollary 4. *Suppose M is a finitely generated A-module, $\mathfrak{a} \trianglelefteq A$, and $M = \mathfrak{a}M$. Then there is $a \in A$ such that $aM = 0$ and $a \equiv 1 \pmod{\mathfrak{a}}$.*

Proof. Suppose $a_i \in \mathfrak{a}$ are the ones given by Proposition 3 for $\phi := \mathrm{Id}_M$. Let $a := 1 + \sum_{i=0}^{n-1} a_i$. Then $\mathrm{Id}_M + \overline{a}_{n-1}\mathrm{Id}_M + \cdots + \overline{a}_0 = 0$ implies that $aM = 0$; and clearly $a \equiv 1 \pmod{\mathfrak{a}}$. □

Lemma 5 (Nakayama's lemma)**.** *Suppose M is a finitely generated A-module. If $J(A)M = 0$, then $M = 0$.*

Proof. By the previous corollary there is $a \in A$ such that $aM = 0$ and $a \equiv 1 \pmod{J(A)}$. So $a \in 1 + J(A) \subseteq A^{\times}$. Therefore $aM = 0$ implies that $M = 0$. □

Primary ideals

We would like to have a general version of prime factorization at least for ideals. It turns out that instead of using powers of primes ideals, we have to work with *primary* ideals.

Definition 6. *We say $\mathfrak{q} \trianglelefteq A$ is a* primary ideal *if $\mathfrak{q}$ is a proper ideal and $xy \in \mathfrak{q}$ implies that either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some positive integer n.*

Lemma 7. *Suppose $\mathfrak{q}$ is a proper ideal of A; $\mathfrak{q} \trianglelefteq A$ is a primary ideal if and only if any zero-divisor of $A/\mathfrak{q}$ is nilpotent.*

Proof. ($\Rightarrow$) Suppose $\overline{x} \in D(A/\mathfrak{q})$ where $D(A/\mathfrak{q})$ is the set of zero-divisors of $A/\mathfrak{q}$. Then there is $\overline{y} \in A/\mathfrak{q} \setminus \{0\}$ such that $\overline{xy} = 0$; that means $y \notin \mathfrak{q}$ and $xy \in \mathfrak{q}$. Since $\mathfrak{q}$ is primary, we deduce that $x^n \in \mathfrak{q}$ for some positive integer n. Hence $\overline{x}^n = 0$ in $A/\mathfrak{q}$, which means $\overline{x}$ is nilpotent in $A/\mathfrak{q}$.

($\Leftarrow$) Suppose $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$. Then $\overline{xy} = 0$ in $A/\mathfrak{q}$ and $\overline{x} \neq 0$. Hence $\overline{y} \in D(A/\mathfrak{q})$, which implies that there is a positive integer n such that $\overline{y}^n = 0$. Therefore $y^n \in \mathfrak{q}$.

(Here $\overline{z} := z + \mathfrak{q}$ for any $z \in A$.) □

Lemma 8. *If $\mathfrak{q}$ is primary, then $\sqrt{\mathfrak{q}} = \mathfrak{p}$ is a prime ideal; and so $\sqrt{\mathfrak{q}}$ is the smallest prime divisor of $\mathfrak{q}$.*

Proof. Suppose to the contrary that there are $x, y \in A$ such that $x, y \notin \sqrt{\mathfrak{q}}$ and $xy \in \sqrt{\mathfrak{q}}$. Then for some positive integer n, $(xy)^n \in \mathfrak{q}$ and $x^n \notin \mathfrak{q}$. Since $\mathfrak{q}$ is primary, there is a positive integer m such that $(y^n)^m \in \mathfrak{q}$. This implies that $y \in \sqrt{\mathfrak{q}}$, which is a contradiction.

Since $\mathfrak{p} := \sqrt{\mathfrak{q}} = \bigcap_{\mathfrak{p}' \in V(\mathfrak{q})} \mathfrak{p}'$, we have that $\mathfrak{p} \subseteq \mathfrak{p}'$ for any $\mathfrak{p}' \in V(\mathfrak{q})$. As $\mathfrak{p} \in V(\mathfrak{q})$, we have that $\mathfrak{p}$ is the smallest prime divisor of $\mathfrak{q}$. □

Definition 9. *A primary ideal* $\mathfrak{q}$ *is called* $\mathfrak{p}$-primary *if* $\sqrt{\mathfrak{q}} = \mathfrak{p}$.

The converse of the above lemma does not hold in general; but if $\sqrt{\mathfrak{q}}$ is a maximal ideal, then we can deduce that $\mathfrak{q}$ is primary.

Lemma 10. *If* $\mathfrak{m} \in \mathrm{Max}(A)$ *and* $\sqrt{\mathfrak{q}} = \mathfrak{m}$, *then* $\mathfrak{q}$ *is* $\mathfrak{m}$*-primary.*

Proof. Since $\sqrt{\mathfrak{q}} = \bigcap_{\mathfrak{p} \in V(\mathfrak{q})} \mathfrak{p} = \mathfrak{m}$, we have that $\mathfrak{q} \subseteq \mathfrak{p} \Rightarrow \mathfrak{m} \subseteq \mathfrak{p}$. Since $\mathfrak{m}$ is a maximal ideal, we have $V(\mathfrak{q}) = \{\mathfrak{m}\}$.

We will continue in the next lecture. □