Lecture 3

1. Review of basic facts on ideals

Definition 1.1. *Let $P \leq A$ be a proper ideal. Then P is a* **prime ideal** *if whenever $ab \in P$, we have $a \in P$ or $b \in P$.*

Proposition 1.2. *Let $\phi : A \to A'$ a ring homomorphism.*

(1) *If P' is prime in A' then $\phi^{-1}(P') = P$ is prime in A;*
(2) *If ϕ is surjective, P is prime in A, and $\ker\phi \subseteq P$ then $\phi(P) = P'$ is prime in A'.*
Generally, $\phi^{-1}(P')$ is denoted by $P' \cap A$.

Proof. For (a), let $ab \in \phi^{-1}(P')$. Then $\phi(ab) \in P'$, and $\phi(ab) = \phi(a)\phi(b)$, so either $\phi(a) \in P'$ or $\phi(b) \in P'$, so either $a \in \phi^{-1}(P')$ or $b \in \phi^{-1}(P')$.

For (b), let $a'b' \in A' \cap \phi(P)$. Then ϕ is surjective so $\exists\, a, b \in A$ such that $\phi(a) = a'$ and $\phi(b) = b'$. Also, $\phi(a)\phi(b) = \phi(ab) \in \phi(P)$ implies $\phi(ab) = \phi(p)$ for some $p \in P$. Thus $ab - p \in \ker\phi \subseteq P$ so $ab \in P$. Thus $a \in P$ or $b \in P$ which implies $a' = \phi(a) \in \phi(P)$ or $b' = \phi(b) \in \phi(P)$. $\square$

In general, for any surjective ring homomorphism $\phi : A \to A'$, we have that $A' \simeq \dfrac{A}{\ker\phi}$ by the Fundamental Isomorphism Theorem, and ideals in I in A' have the form $I = \dfrac{J}{\ker\phi}$ with $J \leq A$ and $\ker\phi \subseteq J$. Moreover, the assignment $I \to J$ is an one-to-one corespondence between ideals of A' and ideals of A containing $\ker\phi$.

Remark 1.3. Take ${}_AM$ and $I \leq A$ such that $IM = 0$. Then M is an A/I-module and M has the same module structure as M over A. Namely, the A/I-module structure on M is defined as follows: if $\overline{a} \in A/I$, $\overline{a}m := am$. This is well defined since if $\overline{a} = \overline{b}$ then $a - b \in I$, but $(a-b)m = 0$ so $am = bm$.

We often consider $\mathcal{L}_A(M)$, the lattice of A-submodules of M. In the case $IM = 0$, this is the same as $\mathcal{L}_{A/I}(M)$ by the above remark.

Corollary 1.4. (1) *P is a prime ideal in A if and only if A/P is a domain;*
(2) *(0) is a prime ideal if and only if A is a domain;*
(3) *Let $R \subseteq S$. If S is a domain then so is R.*

Proof. Simple exercise. $\square$

Let $(P, \leq)$ be a partially ordered set. A chain of elements in P is a sequence $\{a_i\}_{i \in I}$ such that for all $i, j \in I$ either $a_i \leq a_j$ or $a_j \leq a_i$. A subset of P, say S admits an upper bound if $\exists\, x \in P$ such that $x \leq x$ for every $x \in S$.

Lemma 1.5. *(Zorn's Lemma) If P is a partially ordered set such that every non-empty subset of P that is totally ordered admits an upper bound, then P has a maximal element, i.e., $\exists\, x \in P$ such that if $x \leq y$ then $x = y$. In fact, for each $a \in P$, one can find a maximal element X with $a \leq X$.*

Theorem 1.6. *(Krull) If ${}_AM$ is finitely generated and L is a proper submodule of M, then there is a maximal proper submodule of M, say N, with $L \leq N$.*

Proof. We shall just sketch the main ideas. Let $P = \{N : N \leq M, N \neq M, L \subset N\}$ and consider $(P, \subseteq)$. Note that $L \in P$.

We need to show that every nonempty totally ordered subset of P has an upper bound. Let $\{N_i\}_{i \in I}$ be a chain in P. Then $N = \bigcup_{i \in I} N_i$ is an A-submodule of M, as it can be checked easily. It contains L.

It is proper since M is finitely generated: If $M = Ax_1 + \ldots + Ax_n$ and $N = M$, there exists $i \in I$ containing all $x_1, \ldots, x_n$, by the chain condition, which in turn leads to $N_i = M$. This is impossible, so N is proper too.

Therefore, Zorn's Lemma can be applied and we obtain a maximal proper submodule of M containing L.

$\square$

Corollary 1.7. *Every ring has a maximal ideal.*

Proposition 1.8. *Let $\phi : A \to A'$ be a surjective homomorphism of rings. Then the following are true:*

(1) *If $\mathfrak{m}'$ is a maximal ideal in A' then $m' \cap A = \phi^{-1}(\mathfrak{m}')$ is maximal in A;*
(2) *If $\mathfrak{m}$ is maximal in A and $\mathfrak{m} \supseteq \ker \phi$ then $\phi(\mathfrak{m})$ is maximal in A'.*

Proof. This follows from the Correspondence Theorem for quotiens and considering $A \to \dfrac{A}{\ker \phi}$. $\square$

Proposition 1.9. *An ideal $\mathfrak{m}$ is maximal in A if and only if $A/\mathfrak{m}$ is a field.*

Definition 1.10. *If A is a ring then the Jacobian radical of A is the intersection of all maximal ideals in A. This is denoted by $Jac(A)$ (or $Rad(A)$ or $J(A)$).*

Definition 1.11. *A* **local ring** *is a ring A with a unique maximal ideal. Sometimes in recent literature this definition includes the Noetherian condition. In that context, a quasi-local ring is a local ring not necessarily Noetherian. In our notes, we do not assume that the Noetherian condition is part of the definition of a local ring.*

A **nonzerodivisor (NZD)** *on an A-module M is an element $0 \neq a \in A$ with the property that $am = 0$, $m \in M$ implies $m = 0$.*

Let A be a domain. An A-module M is called torsion-free if $am = 0$, for $a \neq 0, a \in A, m \in M$ implies $m = 0$.

2. Krull's Intersection Theorem

Theorem 2.1. *(Krull's Intersection Theorem) Let A be Noetherian, $I \leq A$, ${}_AM$ finitely generated, and take $L = \bigcap_{n=1}^{\infty} I^n M$. Then $I \cdot L = L$.*

Proof. First note that the module M is Noetherian over A. So we can find a submodule N of M that is maximal with property that $N \cap L = IL$. First we will show that there is n such that $I^n M \subseteq N$:

Let $a \in I$ and let $P_i = \{x \in M : a^i x \in N\}$ which can be easily checked that it is an A-submodule of M. The family of $\{P_i\}$ forms an ascending chain condition in M so it must stabilize; there exists m such that $P_m = P_{m+1} = ...$ We claim that $(a^m M + N) \cap L = IL$. Note that $IL \subset L, IL \subset N \subset a^m M + n$. Now let $z \in (a^m M + N) \cap L$. Then $z = a^m x + y$ with $x \in M$ and $y \in N$ and moreover $z \in L$. So, $az \in aL \subset IL \subset N$ and this implies that $a^{m+1} x \in N$, that is $x \in P_{m+1} = P_m$. In conclusion $a^m x \in N$ and this shows that $z \in N$, since $z = a^m x + y, y \in N$. But $N \cap L = IL$ and this gives that $z \in IL$. So, our claim is true, and in particular $a^m M + N = N$, by maximality of N and hence $a^m M \subseteq N$.

Let $I = (a_1, ..., a_h)$ and m_i integers, for $i = 1, ..., h$, such that $a_i^{m_i} M \subseteq N$. For $n = m_1 + \cdots + m_r$, we see that $I^n M \subseteq N$.

To finish the proof, let us remark that $L \subseteq I^n M \subseteq N$ and hence $L = N \cap L = IL$.

□

Lemma 2.2. *Let $I \leq A$, ${}_AM$ finitely generated by n elements. If $a \in A$ such that $aM \subseteq IM$, then $\exists\, b \in I$ such that $(a^n + b)M = 0$.*

Proof. Let $M =_A \langle x_1, ..., x_n \rangle$, with $x_i \in M$. Then for every i, $ax_i = \sum_{j=1}^{n} a_{ij} x_j$ with $a_{ij} \in I$. Set $A = (a_{ij}) \in M_n(A)$. Note that $(a \cdot I_n - A) \cdot X = 0$ where X is the column vector of the x_i's, and I_n is the $n \times n$ identity matrix. Conclude that $\det(aI_n - A)X = 0$. Thus $\det(aI_n - A) \cdot M = 0$ because if an element kills every generator of M, then it kills M also. But, by using the definition of the determinant, we see that we can write $\det(aI_n - A) = a^n + b$ where b is a sum of terms each containing some $a_{ij} \in I$ and hence b belongs to I. □

Corollary 2.3. *If $I \leq A$, ${}_AM$ finitely generated and $IM = M$ then $\exists\, b \in I$ such that $(1+b)M = 0$.*

Proof. Set $a = 1$ in the above lemma. □

The following lemma is important in the study of commutative rings and is a corollary of the statement above:

Lemma 2.4. *(NAK Lemma) If M is a finitely generated module over A, $I \subseteq Jac(A)$, and $IM = M$, then $M = 0$.*

Proof. By the Corollary above, we have that there exists $b \in I$ such that $(1+b)M = 0$. But, since $I \subseteq \mathrm{Jac}(A) = \bigcap \mathfrak{m}$, where the intersection is taken over all maximal ideals $\mathfrak{m}$ of A, it follows that $1+b \notin \mathfrak{m}$ for any $\mathfrak{m}$ maximal ideal of A (otherwise, $1 = 1+b-b \in \mathfrak{m}$, for some $\mathfrak{m}$ maximal ideal of A). Therefore $1+b$ is invertible in A and so $M = 0$.

□

Corollary 2.5. *Let A be a Noetherian domain, and ${}_AM$ be finitely generated and torsion free. Take $I \leq A$. Then $\bigcap_{n=1}^{\infty} I^n M = 0$.*

Proof. First apply Krull's theorem. Then $L = \bigcap_{n=1}^{\infty} I^n M$ and $IL = L$. By the previous corollary, $\exists\, b \in I$ such that $(1+b)L = 0$ which implies $L = 0$, since M is torsion-free. □

Corollary 2.6. *Let A be Noetherian, $I \leq A$, $I \subseteq Jac(A) = \bigcap \mathfrak{m}$ over all maximal ideals $\mathfrak{m}$ of A, and ${}_AM$ be finitely generated. Then $\bigcap_{n=1}^{\infty} I^n M = 0$.*

Proof. As before, proceed to $L = \bigcap_{n=1}^{\infty} I^n M$ and $(1+b)L = 0$ for some $b \in I$. Note that $1+b$ is a unit in A because $1+b$ is not in any maximal ideal of A. Thus $L = 0$. □