

Algebra 557: Week 1

Throughout this course by a ring A we will understand a commutative ring with 1.

1 Rings and Modules.

1.1 Maximal and Prime Ideals, Chinese Remainder Theorem.

We recall the definitions of ideals, ring homomorphisms, unit (invertible) elements, proper ideals, maximal ideals and prime ideals.

Theorem 1. *If I is a proper ideal of a ring A then there exists at least one maximal ideal containing I .*

Definition 2. *An ideal $P \subset A$ for which the quotient A/P is an integral domain is called a prime ideal. Equivalently, an ideal P is prime if it satisfies*

- $P \neq A$,
- $x, y \notin P \Rightarrow xy \notin P$.

An easy consequence of the above definition is

Theorem 3. *If I, J are ideals of A and P a prime ideal, then $I \not\subset P, J \not\subset P \Rightarrow IJ \not\subset P$.*

Definition 4. *A subset $S \subset A$ is called a **multiplicative subset** if it satisfies*

- $x, y \in S \Rightarrow xy \in S$, and
- $1 \in S$.

Theorem 5. *Let S be a multiplicative subset and $I \subset A$ an ideal disjoint from S ; then there exists a prime ideal $P \supset I$ which is disjoint from S .*

Proof. By Zorn's lemma there exists an ideal P which is maximal amongst the ideals containing I and disjoint from S . We claim that P is prime. Suppose that $x, y \notin P$. Then, $P + xA, P + yA$ both meet S , and hence their product $(P + xA)(P + yA)$ also meets S since S is multiplicative. But $(P + xA)(P + yA) = P + xyA$, which implies that $xy \notin P$, proving that P is prime. \square

Definition 6. *The **radical** of an ideal I (written \sqrt{I}) is defined by*

$$\sqrt{I} = \{a \in A \mid a^n \in I \text{ for some } n > 0\}.$$

Theorem 7.

$$\sqrt{I} = \bigcap_{P \supset I, P \text{ prime}} P.$$

Proof. If P is a prime ideal containing I , and $a^n \in I \subset P$, then $a \in P$. Thus, $\sqrt{I} \subset P$. Conversely, if $x \notin \sqrt{I}$, then the multiplicative set $S_x = \{1, x, x^2, x^3, \dots\}$ is disjoint from I . By previous theorem there exists a prime ideal P containing I but disjoint from S . In particular, $x \notin P$, implying that $\sqrt{I} = \bigcap_{P \supset I, P \text{ prime}} P$. \square

Definition 8. $\sqrt{(0)}$ is called the *nilradical* of A (denoted $\text{nil}(A)$). Clearly,

$$\text{nil}(A) = \bigcap_{P \text{ prime ideal of } A} P.$$

If $\text{nil}(A) = 0$ we call the ring A to be *reduced*. Otherwise, we denote by A_{red} the reduced ring $A/\text{nil}(A)$.

Definition 9. A ring A having only one maximal ideal \mathfrak{m} is called a *local ring*. The field $k = A/\mathfrak{m}$ is called the *residue field* (and we denote such a local ring by the triple (A, \mathfrak{m}, k)). A ring having a finite number of maximal ideals will be called *semi-local*.

Definition 10. The *Jacobson radical* of A (denoted $\text{rad}(A)$) is defined as the ideal of A which is the intersection of all its maximal ideals.

The Jacobson radical can be characterized by the following property.

Theorem 11. An element $x \in \text{rad}(A)$ if and only if $1 + ax$ is a unit for each $a \in A$.

Proof. Suppose $x \in \text{rad}(A)$ and $a \in A$. Let \mathfrak{m} be the maximal ideal containing $1 + ax$. Then, $x \in \mathfrak{m}$. But then $1 \in \mathfrak{m}$. Hence, $(1 + ax) = (1)$.

Conversely, suppose that $1 + ax$ is invertible for each $a \in A$, and let \mathfrak{m} be a maximal ideal. Then if $x \notin \mathfrak{m}$, we will have $1 \in \mathfrak{m} + (x)$, and thus $1 = m - ax$, for some $m \in \mathfrak{m}$, and $a \in A$. This would imply that m is a unit. \square

1.2 Chinese Remaindering

In general for any two ideals I, J , the product IJ is contained in $I \cap J$ but not necessarily equal to it. Equality holds if $I + J = A$ (in which case we say I, J are *co-prime*).

Lemma 12. If $I + J = 1$ then $IJ = I \cap J$.

Proof. In this case $I \cap J = (I \cap J)(I + J) \subset IJ \subset I \cap J$. \square

Lemma 13. If I, J are coprime and I, K are co-prime then I is co-prime to JK .

Proof. $(1) = (I + J)(I + K) = I + JK$. \square

By induction we obtain

Theorem 14. If I_1, I_2, \dots, I_n are co-prime in pairs then

$$I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n.$$

Remark 15. In particular, if A is a semi-local ring and $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ are its maximal ideals then

$$\text{rad}(A) = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cdots \mathfrak{m}_n.$$

We also have

Theorem 16. (*Chinese Remainder*) If I_1, I_2, \dots, I_n are co-prime in pairs then

$$A/I_1 \cdots I_n \cong A/I_1 \times \dots \times A/I_n.$$

1.3 Modules.

1.3.1 Basic Definitions.

Definition 17. An A -module M is an abelian group under addition, along with a left-multiplication by elements of A satisfying:

- $a(x + y) = ax + by$
- $(ab)x = a(bx)$
- $(a + b)x = ax + bx$
- $1x = x$.

Definition 18. Let N, N' be sub-modules of M . Then we denote by

$$(N : N')_A = \{a \in A \mid aN' \subset N\}$$

(note that $(N : N')_A$ is an ideal of A).

Similarly, given an ideal $I \subset A$, we will denote

$$(N : I)_M = \{m \in M \mid Im \subset N\}$$

which is a sub-module of M (called the *colon-quotient*).

Finally, the *annihilator* of a module M (denoted by $\text{ann}(M)$) is the ideal $(0 : M)_A$.

We call a module M *faithful* if $\text{ann}(M) = 0$.

1.3.2 Determinant trick, Nakayama lemma and applications.

Theorem 19. Let M be a finitely generated A -module generated by n elements and let $\phi \in \text{Hom}_A(M, M)$. Let I be an ideal of A with $\phi(M) \subset IM$. Then there exists a relation of the form

$$\phi^n + a_1\phi^{n-1} + \dots + a_{n-1}\phi + a_n = 0,$$

with $a_i \in I^i, 1 \leq i \leq n$ (both sides considered as elements of $\text{Hom}_A(M, M)$).

Proof. Cramer's rule. □

Theorem 20. (*Nakayama's Lemma*) Let M be a finitely generated A -module and $I \subset A$ an ideal of A , such that $M = IM$. Then, there exists $a \in A$, with $a \equiv 1 \pmod{I}$, such that $aM = 0$. In particular, if $I \subset \text{rad}(A)$, then $M = 0$.

Proof. Take in the previous theorem $\phi = \text{Id}_M$. Then the obtained relation has the form

$$1 + a_1 + \cdots + a_n = 0$$

and choose for $a = 1 + a_1 + \cdots + a_n$. \square

Theorem 21. *Let M be an A -module and N a sub-module such that M/N is finitely generated. Let $I \subset \text{rad}(A)$ be an ideal such that $M = N + IM$. Then, $M = N$.*

Proof. Let $M' = M/N$. Then $IM' = M'$, and by previous theorem $M' = 0$. \square

Theorem 22. *If A is a local ring and M a f.g. A -module, then every minimal generating set of M has the same number of elements.*

Proof. Choose a basis $\bar{u}_1, \dots, \bar{u}_n \in M/\mathfrak{m}M$ of the k -vector space $M/\mathfrak{m}M$, and lift each vector \bar{u}_i to an element $u_i \in M$. We claim that u_1, \dots, u_n generate M . Let $N = \sum_{1 \leq i \leq n} Au_i$. Then

$$M = N + \mathfrak{m}M.$$

Applying Nakayama (Theorem 20), we have that $M = N$.

Conversely, any minimal generating set of M is of the above form. If $u_1, \dots, u_n \in M$ is a minimal generating set, then clearly $\bar{u}_1, \dots, \bar{u}_n \in M/\mathfrak{m}M$ span $M/\mathfrak{m}M$. We claim that in fact they form a basis. Indeed if any proper subset of these vectors spanned, then by the above argument their inverse images would generate M contradicting the minimality of the generating set. \square

Theorem 23. *Let M be a f.g. A module and $f \in \text{Hom}_A(M, M)$ a surjective homomorphism. Then f is injective as well.*

Proof. Consider the $A[X]$ -module structure on M given by $Xm = f(m)$ for all $m \in M$. Then, $(X)M = M$, and hence by Nakayama (Theorem 20) there exists $F \in A[X]$ such that $(1 + XF)M = 0$. If $u \in \ker f$, then we have that

$$0 = (1 + XF)u = u + F(X(u)) = u + 0 = u.$$

\square