COMMUTATIVE ALGEBRA

M. ATIF ZAHEER

Contents

1. Rings and ideals

1.1. Ideals and ring homomorphisms.

Definition 1.1. Let A be a ring. A subset $\mathfrak{a}$ of A is said to be an *ideal* of A if $\mathfrak{a}$ is an additive subgroup of A and $\mathfrak{a}x \subset \mathfrak{a}$ for every $x \in A$.

Proposition 1.2. Let A be a ring and let $\mathfrak{a}$ be an additive subgroup of A. Then $\mathfrak{a}$ is an ideal of A if and only if the multiplication operation

$$(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}$$

on the quotient group $A/\mathfrak{a}$ is well-defined.

Proposition 1.3 (characterization of ideals in a quotient ring)**.** Let A be a ring and let $\mathfrak{a}$ be an ideal of A. Then there is an inclusion preserving bijective correspondence between the ideals $\mathfrak{b}$ of A containing $\mathfrak{a}$ and the ideals of $A/\mathfrak{a}$ given by $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$.

If $\pi : A \to A/\mathfrak{a}$ is the canonical projection map, then the inverse of the map $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ above is given by $\overline{\mathfrak{b}} \mapsto \pi^{-1}(\overline{\mathfrak{b}})$.

Claim 1.4. Images and preimages of subrings are subrings under a ring homomorphism.

Claim 1.5. Preimage of an ideal under a ring homomorphism is an ideal. The image of an ideal is an ideal of the image ring.

The image of an ideal need not be an ideal. Consider the embedding $\mathbb{Z} \to \mathbb{Q}$.

Theorem 1.6 (Isomorphism theorems)**.**

(a) Let $f : A \to B$ be a ring homomorphism. Then $A/\ker f \cong \operatorname{im} f$.

(b) Let $\mathfrak{a}$ be an ideal and let B be a subring of A. Then $B + \mathfrak{a}$ is a subring of A, $B \cap \mathfrak{a}$ is an ideal of B and

$$(B + \mathfrak{a})/\mathfrak{a} \cong B/(B \cap \mathfrak{a}).$$

(c) If $\mathfrak{a} \subset \mathfrak{b}$ are ideals of a ring A, then

$$(A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \cong A/\mathfrak{b}.$$

1.2. **Zero-divisors, nilpotents, and units.**

Claim 1.7. The set of zero-divisors and units are disjoint.

A nilpotent is always a zero-divisor in a nonzero ring but the converse is not true as $\overline{3} \in \mathbb{Z}/6\mathbb{Z}$ and $\overline{x} \in k[x, y]/(xy)$ are both zero-divisors but not nilpotents.

Problem 1.1. Identify nilpotent elements in the ring $\mathbb{Z}/n\mathbb{Z}$.

Solution. An element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if $\prod_{p|n} p$ divides a.

Proposition 1.8. Let A be a ring $\neq 0$ Then the following are equivalent:
(a) A is a field.
(b) The only ideals of A are 0 and (1).
(c) Every nonzero ring homomorphism from A to a ring B is injective.

1.3. **Prime and maximal ideals.**

Definition 1.9. Let A be a ring. A proper ideal $\mathfrak{p}$ of A is said to be *prime* if $xy \in A$ implies $x \in A$ or $y \in A$.

Example 1.10. (1) If A is an integral domain, then 0 is a prime ideal of A.
(2) The prime ideals of $\mathbb{Z}$ are precisely the zero ideal and ideals of the form (p), where p is a prime number.
(3) The ideal $(x) \subset k[x, y]$ is prime.

Proposition 1.11. An ideal $\mathfrak{p}$ of a ring A is prime if and only if $A/\mathfrak{p}$ is an integral domain.

Claim 1.12. If $f : A \to B$ is a ring homomorphism and $\mathfrak{q}$ is a prime ideal of B, then the inverse image $f^{-1}(\mathfrak{q})$ is also prime.

Proof. The proof is quite simple following directly from the definition but a more instructive proof is as follows: Consider the map $\pi \circ f : A \to B/\mathfrak{q}$, where $\pi : B \to B/\mathfrak{q}$ is the canonical projection. Then $\ker(\pi \circ f) = f^{-1}(\mathfrak{q})$. Thus we have $A/f^{-1}(\mathfrak{q}) \cong (\pi \circ f)(A)$. Since $B/\mathfrak{q}$ is an integral domain, it follows that the subring $(\pi \circ f)(A)$ and hence $A/f^{-1}(\mathfrak{q})$ is an integral domain. This implies that $f^{-1}(\mathfrak{q})$ is prime in A. $\square$

Claim 1.13. Let $f : A \to B$ be a surjective ring homomorphism and let $\mathfrak{p}$ be a prime ideal of A such that $\mathfrak{p} \supset \ker f$. Then the image $f(\mathfrak{p})$ is prime in B.

Definition 1.14. Let A be a ring. A proper ideal $\mathfrak{m}$ of A is said to be *maximal* if there is no proper ideal strictly containing $\mathfrak{m}$.

Proposition 1.15. An ideal $\mathfrak{m}$ of A is maximal if and only if $A/\mathfrak{m}$ is a field.

The inverse image of a maximal ideal need not be maximal. Consider the embedding $\mathbb{Z} \to \mathbb{Q}$. However, the image of a maximal ideal under a surjective ring homomorphism containing the kernel is a maximal ideal.

Theorem 1.16. Every nonzero ring A has a maximal ideal.

Proof. Follows from Zorn's lemma. □

Corollary 1.17. If $\mathfrak{a}$ is a proper ideal of a ring A, then there is a maximal ideal of A containing $\mathfrak{a}$.

Corollary 1.18. Every nonunit element is contained in some maximal ideal.

Problem 1.2. Let A be a ring in which every element x satisfies $x^n = x$ for some $n > 1$. Show that every prime ideal is maximal.

Solution. Let $\mathfrak{p}$ be a prime ideal of A. Then we know that $\mathfrak{p}$ is contained in some maximal ideal $\mathfrak{m}$ of A. Suppose for the sake of contradiction that $\mathfrak{p}$ is properly contained in $\mathfrak{m}$ and let $x \in \mathfrak{m}\backslash\mathfrak{p}$. Then we have $x^n = x$ for some $n > 1$ and so $x(x^{n-1} - 1) = 0 \in \mathfrak{p}$. This implies that $x^{n-1} - 1 \in \mathfrak{p}$ as $x \notin \mathfrak{p}$. It now follows that $x^{n-1} - 1 \in \mathfrak{m}$ as $\mathfrak{p} \subset \mathfrak{m}$. Finally, we get that $1 \in \mathfrak{m}$ as $x \in \mathfrak{m}$, a contradiction. Hence we must have $\mathfrak{p} = \mathfrak{m}$.

Another solution: Let $\mathfrak{p}$ be a prime ideal of A. Then $A/\mathfrak{p}$ is an integral domain. Let $x \in A$. Then $x^n = x$ for some $n > 1$ and so $\overline{x}^n = \overline{x}$. If $\overline{x} \neq 0$, then $\overline{x}^{n-1} = \overline{1}$ and so $\overline{x}$ is a unit. This shows that $A/\mathfrak{p}$ is a field and so $\mathfrak{p}$ is a maximal ideal.

Claim 1.19. If $\mathfrak{m}$ is a proper ideal of a ring A such that $A\backslash\mathfrak{m} \subset A^\times$, then $\mathfrak{m}$ is the unique maximal ideal of A.

Proof. Every proper ideal $\mathfrak{a}$ is contained in $A\backslash A^\times \subset \mathfrak{m}$. □

Claim 1.20. If $\mathfrak{m}$ is a maximal ideal of A such that $1 + \mathfrak{m} \subset A^\times$, then $\mathfrak{m}$ is the unique maximal ideal of A.

Proof. If x is a nonunit element not contained in $\mathfrak{m}$, then $\mathfrak{m} + (x) = (1)$ and so $x \in 1 + \mathfrak{m} \subset A^\times$, a contradiction. □

Problem 1.3. Show that the only idempotents in a local ring are 0 and 1.

Solution. Let x be an idempotent element in a ring A and $\mathfrak{m}$ be the unique maximal ideal of A. Then $x^2 = x$ and so $x(x-1) = 0$. Because $\mathfrak{m} = A\backslash A^\times$ we get that either x or $1 - x$ is a unit for if both are nonunits, then both lie in $\mathfrak{m}$ which results in $1 \in \mathfrak{m}$, a contradiction. This implies that $x = 0$ or $x = 1$.

Claim 1.21. In a PID every nonzero prime ideal is maximal.

1.4. **Nilradical and Jacobson radical.**

Claim 1.22. The set $\mathfrak{N}$ of all nilpotent elements in a ring A form an ideal. Moreover, the ring $A/\mathfrak{N}$ does not have any nonzero nilpotent elements.

Theorem 1.23. Let A be a ring. Then

$$\mathfrak{N} = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}.$$

Proof. The inclusion $\subset$ is easy. For the other inclusion let $x \in \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}$. Suppose for the sake of contradiction that x is not nilpotent. Then the collection of all ideals $\mathfrak{a}$ of A for which $x^n \notin \mathfrak{a}$ for every $n \in \mathbb{N}$ has a maximal element $\mathfrak{p}$ by the Zorn's lemma. It is then easy to see that $\mathfrak{p}$ is a prime ideal and so we obtain a contradiction. □

Problem 1.4. Let A be a ring and let $\mathfrak{N}$ be its nilradical. Show that the following are equivalent:

(a) A has exactly one prime ideal.
(b) Every element of A is either a unit of a nilpotent.
(c) $A/\mathfrak{N}$ is a field.

Solution. (a) $\Rightarrow$ (b): Let $x \in A$ be a nonunit. Then x lies in some prime ideal $\mathfrak{p}$ of A. But by assumption $\mathfrak{p}$ is the unique prime ideal of A and so $\mathfrak{N} = \mathfrak{p}$. Thus x is a nilpotent.

(b) $\Rightarrow$ (c): By assumption we have $A \backslash A^\times \subset \mathfrak{N}$. This immediately shows that $\mathfrak{N}$ is the unique maximal ideal of A by Claim 1.19 and so $A/\mathfrak{N}$ is a field.

(c) $\Rightarrow$ (a): If $\mathfrak{p}$ is a prime ideal of A, then $\mathfrak{N} \subset \mathfrak{p}$. Since $\mathfrak{N}$ is a maximal ideal we get that $\mathfrak{p} = \mathfrak{N}$. Hence, $\mathfrak{N}$ is the unique prime ideal of A.

Theorem 1.24. Let $\mathfrak{R}$ be the Jacobson radical of a ring A. Then $x \in \mathfrak{R}$ if and only if $1 + xy \in A^\times$ for every $y \in A$.

1.5. **Problems.**

Problem 1.5. Let x be a nilpotent element of a ring A. Show that $1 + x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.

Solution. Take $y = -x$. Then y is also nilpotent. Let $y^n = 0$. Note that

$$1 = 1 - y^n = (1 - y)(1 + y + \cdots + y^{n-1}).$$

This shows that $1 - y = 1 + x$ is a unit. Now if u is a unit, then $u^{-1}x$ is also nilpotent and so it follows that $u(1 + u^{-1}x) = u + x$ is a unit by the previous result.

Problem 1.6. Let A be a ring and let $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. Prove that

(a) f is a unit in $A[x]$ if and only if a_0 is a unit and $a_1, \ldots, a_n$ are nilpotent. (If $g = b_0 + b_1x + \cdots + b_mx^m$ is the inverse of f, prove by induction on r that $a_n^{r+1}b_{m-r} = 0$ and conclude that a_n is nilpotent.)
(b) f is nilpotent if and only if $a_0, a_1, \ldots, a_n$ are nilpotent.
(c) f is a zero divisor if and only if there is a $a \neq 0$ in A such that $af = 0$. (Choose a polynomial $g = b_0 + b_1x + \cdots + b_mx^m$ of least degree m such that $fg = 0$. Then $a_nb_m = 0$, hence $a_ng = 0$ as a_ng annihilates f and has degree $< m$. Now show by induction that $a_{n-r}g = 0$ for every $0 \leqslant r \leqslant n$.)

(d) f is said to be *primitive* if $(a_0, a_1, \dots, a_n) = 1$. Prove that if $f, g \in A[x]$, then fg is primitive if and only if f and g are primitive.

Solution. (a): Let $f = a_n x^n + \cdots + a_1 x + a_0$ be a unit in $A[x]$ and let $g = b_m x^m + \dots b_1 x + b_0$ be such that $fg = 1$. Since the constant term of fg is $a_0 b_0$ we get $a_0 b_0 = 1$ and so a_0 is a unit. We now show that $a_n^{r+1} b_{m-r} = 0$ for $0 \leqslant r \leqslant m$. Clearly we have $a_n b_m = 0$ as it is the coefficient of x^{n+m} in fg. Suppose that $a_n^{s+1} b_{m-s} = 0$ for all $0 \leqslant s < r$, where $r \leqslant m$. Now consider the coefficient of x^{n+m-r} in fg which is given as

$$a_n b_{m-r} + a_{n-1} b_{m-r+1} + \cdots + a_{n-r} b_m = 0$$

if $r \leqslant n$ and

$$a_n b_{m-r} + a_{n-1} b_{m-r+1} + \cdots + a_0 b_{m-r+n} = 0$$

if $r > n$. Multiplying this by a_n^r we get either

$$a_n^{r+1} b_{m-r} + a_{n-1}(a_n^r b_{m-r+1}) + \cdots + a_{n-r} a_n^{r-1}(a_n b_m) = 0$$

or

$$a_n^{r+1} b_{m-r} + a_{n-1}(a_n^r b_{m-r+1}) + \cdots + a_0 a_n^{n-1}(a_n^{r-n+1} b_{m-r+n}) = 0.$$

Because the terms in the parenthesis are all zero by the induction hypothesis we conclude that $a_n^{r+1} b_{m-r} = 0$. Thus $a_n^{r+1} b_{m-r} = 0$ for all $0 \leqslant r \leqslant m$. In particular, we have $a_n^{m+1} b_0 = 0$. Because b_0 is a unit it follows that $a_n^{m+1} = 0$ and so a_n is nilpotent. Since we know that a unit shifted by a nilpotent element stays a unit, we deduce that $h = f - a_n x^n = a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is a unit. Repeating the above argument for h we obtain that a_{n-1} is nilpotent. Continuing this way we conclude that $a_1, \dots, a_n$ are all nilpotent.

For the converse, let f as above and assume that $a_1, \dots, a_n$ are all nilpotent. Then it follows that $a_1 x, \dots, a_n x^n$ are nilpotent as well, which in turn implies that $p = f - a_0 = a_1 x + \cdots + a_n x^n$ is also nilpotent (as the set of nilpotent elements form an ideal). Since a unit shifted by a nilpotent element is again a unit, we get that $f = a_0 + p$ is a unit.

(b): If $a_0, a_1, \dots, a_n$ are nilpotent in A, then so are the monomials $a_0, a_1 x, \dots, a_n x^n$ in $A[x]$ which in turn implies that f is nilpotent (as the set of nilpotent elements is an ideal). Conversely, if f is nilpotent, then so xf. It then follows that $1 + xf$ is a unit. Since the nonconstant coefficients of $1 + xf$ are precisely $a_0, a_1, \dots, a_n$ we conclude that $a_0, a_1, \dots, a_n$ are all nilpotent.

(c): Let $f = a_0 + a_1 x + \cdots + a_n x^n$ be a zero divisor and $g = b_0 + b_1 x + \cdots + b_m x^m$ be the polynomial of least degree m satisfying $fg = 0$. Since $a_n b_m = 0$, it follows that $a_n g$ has degree strictly smaller than m. As $(a_n g) f = a_n (gf) = 0$, we deduce that by the minimality of the degree of g that $a_n g = 0$. Suppose that $a_{n-s} g = 0$ for $0 \leqslant s < r$ where $r \leqslant n$. Then observe that

$$\begin{aligned}
0 = gf &= g(a_n x^n + \cdots + a_{n-r+1} x^{n-r+1} + a_{n-r} x^{n-r} + \cdots + a_1 x + a_0) \\
&= (a_n g) x^n + \cdots + (a_{n-(r-1)} g) x^{n-r+1} + g(a_{n-r} x^{n-r} + \cdots + a_1 x + a_0) \\
&= g(a_{n-r} x^{n-r} + \cdots + a_1 x + a_0).
\end{aligned}$$

The last inequality implies in particular that $a_{n-r}b_m = 0$ and so $a_{n-r}g$ has degree strictly smaller than the degree of g. Because $(a_{n-r}g)f = a_{n-r}(gf) = 0$, it follows by the minimality of degree of g that $a_{n-r}g = 0$. Thus we have shown that $a_{n-r}g = 0$ for $0 \leqslant r \leqslant n$. This gives us $a_{n-r}b_m = 0$ for all $0 \leqslant r \leqslant n$ and so $b_m f = 0$ as desired.

(d): Suppose that $f, g \in A[x]$ are primitive. Let $\mathfrak{a}$ be the ideal of A generated by the coefficients of fg. Let $\overline{f}$ and $\overline{g}$ be the polynomials in $(A/\mathfrak{a})[x]$ obtained from f and g by reducing the coefficients mod $\mathfrak{a}$. By the definition of $\mathfrak{a}$, we have $\overline{f}\overline{g} = \overline{fg} = 0$. If either $\overline{f} = 0$ or $\overline{g} = 0$, then we would be done for this would imply that the coefficients of f or coefficients of g lie in $\mathfrak{a}$ and since f and g are primitive it would follow that $\mathfrak{a} = (1)$. Suppose for the sake of contradiction that $\overline{f} \neq 0$ and $\overline{g} \neq 0$. This implies that $\overline{f}$ is a zero divisor and so by part (c) there is a nonzero $\overline{b} \in A/\mathfrak{a}$ such that $\overline{b}\,\overline{f} = \overline{bf} = 0$. If $f = a_0 + a_1x + \cdots + a_nx^n$, then we have $ba_i \in \mathfrak{a}$ for all i. Since f is primitive, there exist $c_i \in A$ such that

$$\sum_{i=0}^{n} c_i a_i = 1.$$

Multiplying by b we get

$$\sum_{i=0}^{n} c_i(ba_i) = b.$$

Because $ba_i \in \mathfrak{a}$ for each i, it follows that $b \in \mathfrak{a}$, a contradiction as $\overline{b} \neq 0$.

The converse is trivial for the ideal generated by the coefficients of fg is contained in the ideal generated by the coefficients of f and the ideal generated by the coefficients of g and so if fg is primitive, then so are f and g.