

3. COMMUTATIVE RINGS: BASICS

I went over the basic facts about ideals in commutative rings.

3.1. maximal ideals.

Definition 3.1. A *maximal ideal* in a ring R is an ideal which is not properly contained in any other ideal.

Zorn's lemma tells us that all rings have maximal ideals.

Theorem 3.2. Any ideal I in any ring R is contained in a maximal ideal. In particular, R has at least one maximal ideal.

Proof. To prove this we need:

Axiom 3.3 (Zorn's Lemma). If P is a partially ordered set in which every tower has an upper bound, then P has a maximal element.

Partially ordered means it has a transitive, reflexive, antisymmetric relation \leq (so that $a \leq b, b \leq a \Rightarrow a = b$). In this case we are talking about the set of all ideals $J \subset R$ which contain I . A *tower* is a totally ordered subset: i.e., $T = \{J_\alpha\}$ is a tower if for all α, β either $J_\alpha \subseteq J_\beta$ or $J_\beta \subseteq J_\alpha$. If we had such a tower, the union

$$J_\infty = \bigcup J_\alpha$$

is an ideal containing every J_α and not containing 1. Since J_∞ contains each J_α , J_∞ is an upper bound for the tower. So, Zorn's lemma tells us that there is a maximal element in the poset of all ideals containing I . I.e., I is contained in a maximal ideal. \square

Lemma 3.4. A commutative ring is a field if and only if 0 is the only ideal.

Proof. If R is not a field then it has an element $x \neq 0$ which is not invertible. Then $(x) = xR$ is a nonzero ideal. The converse is obvious. \square

Proposition 3.5. An ideal I is maximal if and only if R/I is a field.

Proof. The ideals of R/I all have the form J/I where J is an intermediate ideal, i.e., $I \subseteq J \subset R$. So, I is maximal iff $I/I = 0$ is a maximal ideal in R/I iff R/I is a field. \square

3.2. zero divisors and prime ideals.

Definition 3.6. An ideal P is called *prime* if the complement of P is closed under multiplication, i.e., $a, b \notin P \Rightarrow ab \notin P$.

Definition 3.7. A *zero divisor* is a nonzero element $a \in R$ so that $ab = 0$ for some $b \neq 0$ in R . A ring with no zero divisors is called a *domain* (or *integral domain*). Lang uses the adjective *entire* for this. I.e., a domain is an entire ring.

Example 3.8. If R, S are commutative rings then the Cartesian product $R \times S = \{(r, s) \mid r \in R, s \in S\}$ is a ring with addition and multiplication defined “coordinatewise”:

$$(r, s) + (r', s') = (r + r', s + s')$$

$$(r, s)(r', s') = (rr', ss')$$

This ring has two idempotents:

$$e_1 = (1, 0), \quad e_2 = (0, 1)$$

which are orthogonal: $e_1e_2 = (0, 0) = 0$. These are zero divisors. If a ring has no zero divisors then it does not factor as a product! So, it is “one piece.”

Having no zero divisors is the same as saying that the set of nonzero elements is closed under multiplication. This gives the following.

Proposition 3.9. R is a domain if and only if 0 is a prime ideal.

Corollary 3.10. An ideal I in R is prime if and only if R/I is a domain.

3.3. polynomial rings. If A is any ring, the *polynomial ring* $A[X]$ is defined to be the set of all formal expressions called *polynomials*:

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$$

where $a_i \in A$. The word “formal expression” means that two such elements are equal if and only if they have the same coefficients a_i . Every polynomial gives a function $R \rightarrow R$ given by evaluation. But two polynomials might give the same function!

Suppose that A is a subring of B and $b \in B$. Then the *evaluation map*

$$ev_b : A[X] \rightarrow B$$

is the ring homomorphism given by

$$ev_b(f) = f(b) = a_nb^n + a_{n-1}b^{n-1} + \cdots + a_0.$$

More generally we have the ring of polynomials in several variables: $A[X_1, \dots, X_n]$. This is defined recursively by

$$A[X_1, \dots, X_n] = A[X_1, \dots, X_{n-1}][X_n]$$

In other words, a polynomial in the variables X_1, \dots, X_n is the same as a polynomial in X_n whose coefficients are polynomials in the first $n - 1$ variables.

Polynomial rings satisfy the following universal property.

Proposition 3.11. *If A is a subring of B and $x_1, x_2, \dots, x_n \in B$ then there is a unique ring homomorphism*

$$ev_{(x)} : A[X_1, \dots, X_n] \rightarrow B$$

which is equal to the inclusion map on A and which sends X_i to x_i .

Proof. This is sort of obvious. The homomorphism must be the one which sends $f(X_1, \dots, X_n)$ to $f(x_1, \dots, x_n)$. \square

3.4. Example. I talked about the example $\mathbb{Z}[\sqrt{-5}]$ without complete proofs. We need theorems about PID's and UFD's to do this.

First, I pointed out that if B is a domain then the kernel of any evaluation map

$$\phi = ev_b : A[X] \rightarrow B$$

must be a prime ideal. The image is, by definition, the ring $A[b]$.

I took as an example, $B = \mathbb{C}$, $A = \mathbb{Z}$ and $b = \sqrt{-5}$. The prime ideal in this case is the principal ideal

$$\ker \phi = (X^2 + 5).$$

The image is the ring $\mathbb{Z}[\sqrt{-5}]$. The elements of this ring are

$$a + b\sqrt{-5}$$

where $a, b \in \mathbb{Z}$. The proof is simple. The set of such elements forms a ring and it is clearly the smallest ring containing \mathbb{Z} and $\sqrt{-5}$.

This ring is not a UFR (unique factorization domain) since

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

And it is not a PID since

$$(2, 1 + \sqrt{-5})$$

is not a principal ideal. I.e., it is not equal to (a) for any $a \in R = \mathbb{Z}[\sqrt{-5}]$.

The elements $2, 3, 1 \pm \sqrt{-5}$ are *irreducible* elements of the ring R . This means that for any factorization of these elements, one of the factors will always be a unit. E.g., $2 = ab$ implies either a or b is a unit. The word “irreducible” is used since “prime” is a property of ideals not of numbers.