

18. PRIME AND MAXIMAL IDEALS

Let R be a ring and let I be an ideal of R , where $I \neq R$. Consider the quotient ring R/I . Two very natural questions arise:

- (1) When is R/I a domain?
- (2) When is R/I a field?

Definition-Lemma 18.1. *Let R be a ring and let I be an ideal of R .*

*We say that I is **prime** if whenever $ab \in I$ then either $a \in I$ or $b \in I$.*

Then R/I is a domain if and only if I is prime.

Proof. Suppose that I is prime. Let x and y be two elements of R/I . Then there are elements a and b of R such that $x = a + I$ and $y = b + I$. Suppose that $xy = 0$, but that $x \neq 0$, that is, suppose that $a \notin I$.

$$\begin{aligned} xy &= (a + I)(b + I) \\ &= ab + I \\ &= 0. \end{aligned}$$

But then $ab \in I$ and as I is prime, $b \in I$. But then $y = b + I = I = 0$. Thus R/I is an domain.

Now suppose that R/I is a domain. Let a and b be two elements of R such that $ab \in I$ and suppose that $a \notin I$. Let $x = a + I$, $y = b + I$. Then $xy = ab + I = 0$. As $x \neq 0$, and R/I is an domain, $y = 0$. But then $b \in I$ and so I is prime. \square

Example 18.2. *Let $R = \mathbb{Z}$. Then every ideal in R has the form $\langle n \rangle = n\mathbb{Z}$. It is not hard to see that I is prime iff n is prime.*

Definition 18.3. *Let R be an integral domain and let a be a non-zero element of R . We say that a is **prime**, if $\langle a \rangle$ is a prime ideal, not equal to the whole of R .*

Note that the condition that $\langle a \rangle$ is not the whole of R is equivalent to requiring that a is not a unit.

Definition 18.4. *Let R be a ring. Then there is a unique ring homomorphism $\phi: \mathbb{Z} \rightarrow R$.*

*We say that the **characteristic** of R is n if the order of the image of ϕ is finite, equal to n ; otherwise the characteristic is 0.*

Let R be a domain of finite characteristic. Then the characteristic is prime.

Proof. Let $\phi: \mathbb{Z} \rightarrow R$ be a ring homomorphism. Then $\phi(1) = 1$. Note that \mathbb{Z} is a cyclic group under addition. Thus there is a unique map that

sends 1 to 1 and is a group homomorphism. Thus ϕ is certainly unique and it is not hard to check that in fact ϕ is a ring homomorphism.

Now suppose that R is an integral domain. Then the image of ϕ is an integral domain. In particular the kernel I of ϕ is a prime ideal. Suppose that $I = \langle p \rangle$. Then the image of ϕ is isomorphic to R/I and so the characteristic is equal to p . \square

Another, obviously equivalent, way to define the characteristic n is to take the minimum non-zero positive integer such that $n1 = 0$.

Example 18.5. *The characteristic of \mathbb{Q} is zero. Indeed the natural map $\mathbb{Z} \rightarrow \mathbb{Q}$ is an inclusion. Thus every field that contains \mathbb{Q} has characteristic zero. On the other hand \mathbb{Z}_p is a field of characteristic p .*

Definition 18.6. *Let I be an ideal. We say that I is **maximal** if for every ideal J , such that $I \subset J$, either $J = I$ or $J = R$.*

Proposition 18.7. *Let R be a commutative ring.*

Then R is a field iff the only ideals are $\{0\}$ and R .

Proof. We have already seen that if R is a field, then R contains no non-trivial ideals.

Now suppose that R contains no non-trivial ideals and let $a \in R$. Suppose that $a \neq 0$ and let $I = \langle a \rangle$. Then $I = \{0\}$. Thus $I = R$. But then $1 \in I$ and so $1 = ba$. Thus a is a unit and as a was arbitrary, R is a field. \square

Theorem 18.8. *Let R be a commutative ring.*

Then R/M is a field iff M is a maximal ideal.

Proof. Note that there is an obvious correspondence between the ideals of R/M and ideals of R that contain M . The result therefore follows immediately from (18.7). \square

Corollary 18.9. *Let R be a commutative ring.*

Then every maximal ideal is prime.

Proof. Clear as every field is an integral domain. \square

Example 18.10. *Let $R = \mathbb{Z}$ and let p be a prime. Then $I = \langle p \rangle$ is not only prime, but it is in fact maximal. Indeed the quotient is \mathbb{Z}_p .*

Example 18.11. *Let X be a set and let R be a commutative ring and let F be the set of all functions from X to R . Let $x \in X$ be a point of X and let I be the ideal of all functions vanishing at x . Then F/I is isomorphic to R .*

Thus I is prime iff R is an integral domain and I is maximal iff R is a field. For example, take $X = [0, 1]$ and $R = \mathbb{R}$. In this case it

turns out that every maximal ideal is of the same form (that is, the set of functions vanishing at a point).

Example 18.12. Let R be the ring of Gaussian integers and let I be the ideal of all Gaussian integers $a + bi$ where both a and b are divisible by 3.

I claim that I is maximal. I will give two ways to prove this.

Method I: Suppose that $I \subset J \subset R$ is an ideal, not equal to I . Then there is an element $a + bi \in J$, where 3 does not divide one of a or b . It follows that 3 does not divide $a^2 + b^2$. But

$$c = a^2 + b^2 = (a + bi)(a - bi) \in J,$$

as $a + bi \in J$ and J is an ideal. As 3 does not divide c , we may find integers r and s such that

$$3r + cs = 1.$$

As $c \in J$, $cs \in J$ and as $3 \in I \subset J$, $3r \in J$ as well. But then $1 \in J$ and $J = R$.

Method II: Suppose that $(a + bi)(c + di) \in I$. Then

$$3|(ac - bd) \quad \text{and} \quad 3|(ad + bc).$$

Suppose that $a + bi \notin I$. Adding the two results above we have

$$3|(a + b)c + (a - b)d.$$

Now either 3 divides a and it does not divide b , or vice-versa, or the same is true, with $a + b$ replacing a and $a - b$ replacing b , as can be seen by an easy case-by-case analysis. Suppose that 3 divides a whilst 3 does not divide b . Then $3|bd$ and so $3|d$ as 3 is prime. Similarly $3|c$. It follows that $c + di \in I$. Similar analyses pertain in the other cases. Thus I is prime, so that the quotient R/I is an integral domain. As the quotient is finite (easy check) it follows that the quotient is a field, so that I is maximal. It turns out that R/I is a field with nine elements.

Now suppose that we replace 3 by 5 and look at the resulting ideal J . I claim that J is not maximal. Indeed consider $x = 2 + i$ and $y = 2 - i$. Then

$$xy = (2 + i)(2 - i) = 4 + 1 = 5,$$

so that $xy \in J$, whilst neither x nor y are in J , so that J is not even prime.