Subject : MATHEMATICS

Paper 1 : ABSTRACT ALGEBRA

Chapter 7 : Factorizations in Integral Domains

Module 2 : Prime and irreducible elements

Anjan Kumar Bhuniya
Department of Mathematics
Visva-Bharati; Santiniketan
West Bengal

E-mail: anjankbhuniya@gmail.com

Prime and irreducible elements

Learning Objectives:	1. Introduction of prime and irreducible elements.
	2. Relations between prime and irreducible elements.
	3. $< p >$ is a prime ideal if and only if p is prime.
	4. Irreducibility of the generators of principal maximal ideals.

An integer $p > 1$ is called a prime integer if 1 and p are the only two positive divisors of p. An integer $p > 1$ is prime if and only if $p \mid ab$ implies that $p \mid a$ or $p \mid b$. But this equivalence does not hold in an integral domain in general. In this section the notion of prime integers are generalized into prime elements and irreducible elements in a commutative ring with 1.

Definition 0.1. *Let R be a commutative ring with 1 and p be a nonzero nonunit element of R.*

1. *Then p is called irreducible if for every $a, b \in R$, $p = ab$ implies that either a or b is a unit.*

   p is called reducible if p is not irreducible.

2. *Then p is called prime if for every $a, b \in R$, $p \mid ab$ implies that either $p \mid a$ or $p \mid b$.*

In the ring $\mathbb{Z}$ of all integers, only possible factorizations of 7 are 7×1 and $(-7) \times (-1)$. In each of these factorizations one factor is unit and hence 7 is an irreducible element.

Now for $a, b \in \mathbb{Z}$, $-7 \mid ab$ implies that $7 \mid ab$ and so either $7 \mid a$ or $7 \mid b$. This implies that $-7 \mid a$ or $-7 \mid b$. Thus -7 is a prime element in $\mathbb{Z}$.

Now we give two examples to show that neither every irreducible element is prime nor every prime element is irreducible.

Example 0.2. *Consider the integral domain $\mathbb{Z}[i\sqrt{5}]$ and the element $2 + i\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$. To test irreducibility of $2+i\sqrt{5}$, assume that $2+i\sqrt{5} = (a+ib\sqrt{5})(c+id\sqrt{5})$ for some $a+ib\sqrt{5}, c+id\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$. It follows that $(a^2 + 5b^2)(c^2 + 5d^2) = 9$. Hence we have*

$$a^2 + 5b^2 = 3 \text{ and } c^2 + 5d^2 = 3 \tag{0.1}$$

$$\text{or } a^2 + 5b^2 = 1 \text{ and } c^2 + 5d^2 = 9 \tag{0.2}$$

$$\text{or } a^2 + 5b^2 = 9 \text{ and } c^2 + 5d^2 = 1 \tag{0.3}$$

Equation (0.1) has no solution and from equations (0.2) and (0.3), it follows that $a + ib\sqrt{5} = \pm 1$ or $c + id\sqrt{5} = \pm 1$. Hence $2 + i\sqrt{5}$ is an irreducible element in $\mathbb{Z}[i\sqrt{5}]$.

Now $(2 + i\sqrt{5})(2 - i\sqrt{5}) = 9 = 3 \times 3$ implies that $2 + i\sqrt{5} \mid 3 \times 3$. If $2 + i\sqrt{5} \mid 3$, then $3 = (2+i\sqrt{5})(a+ib\sqrt{5})$ for some $a+ib\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$, which implies that $3 = 2a-5b$ and $a+2b = 0$, and $3 = -9b$, which contradicts $b \in \mathbb{Z}$. Hence $2+i\sqrt{5} \nmid 3$ and so $2+i\sqrt{5}$ is not a prime element in $\mathbb{Z}[i\sqrt{5}]$.

Example 0.3. *Consider the ring* $\mathbb{Z}_6$*. This is a commutative ring with unity* $[1]$*; and the unit elements are* $[1]$ *and* $[5]$*. Since* $[3] = [3][3]$ *and* $[3]$ *is not a unit it follows that* $[3]$ *is reducible.*

Now we show that $[3]$ *is a prime element in* $\mathbb{Z}_6$*. Let* $[a], [b] \in \mathbb{Z}_6$ *be such that* $[3] \mid [a][b]$*. Then* $[a][b] = [3][c]$*, for some* $[c] \in \mathbb{Z}_6$*. This implies that* $6|(ab - 3c)$*. Then* $3|(ab - 3c)$*, and hence* $3|ab$*. Since* 3 *is prime in* $\mathbb{Z}$*,* $3|a$ *or* $3|b$*. Thus either* $[3]|[a]$ *or* $[3]|[b]$ *and hence* $[3]$ *is a prime element in* $\mathbb{Z}_6$*.*

Theorem 0.4. *In an integral domain every prime element is irreducible.*

Proof. Consider an integral domain R and a prime element p in R. Suppose $p = bc$ for some $b, c \in R$. Then $p|bc$ which implies that $p|b$ or $p|c$, since p is prime. If $p|b$, then $b = pq$ for some $q \in R$. Thus, $p = bc = pqc$ and so $p(1 - qc) = 0$. This implies that $1 - qc = 0$, since there is no zero divisors in R and $p \neq 0$. Thus $qc = 1$ showing that c is a unit. Similarly, if $p|c$ then b is a unit. Hence p is irreducible. □

Now we show that prime elements generate prime ideals.

Theorem 0.5. *Let* R *be a commutative ring with 1 and let* $P =< p >$ *be a nonzero ideal of* R*. Then* P *is a prime ideal if and only if* p *is a prime element.*

Proof. First suppose that P is a prime ideal of R. Since P is nonzero and proper, p is neither zero nor a unit. Consider $a, b \in R$ and assume that $p|ab$. Then $ab \in P$ which implies that either $a \in P$ or $b \in P$, since P is a prime ideal. Thus either $p|a$ or $p|b$ and hence p is a prime element.

Conversely, suppose that p is a prime element. Since p is nonunit, so P is a proper ideal of R. Now consider two elements $a, b \in R$ and assume that $ab \in P$. Then $p|ab$ which implies that $p \mid a$ or $p \mid b$, since p is a prime element. Thus either $a \in P$ or $b \in P$ and hence P is a prime ideal of R. □

Theorem 0.6. *Let* D *be an integral domain. If* $M =< q >$ *is a nonzero maximal ideal of* D *then* q *is an irreducible element.*

Proof. Every maximal ideal is, by definition, a proper ideal. Hence q is not a unit. Also q is nonzero, since M is a nonzero ideal. Consider $a, b \in D$ and assume that $q = ab$. Then $q \in< a >$ and so $M =< q >\subseteq< a >$. Hence $M =< a >$ or $< a >= D$, since M is a maximal ideal. If $M =< a >$ then $a \in M$ shows that $a = qc$ for some $c \in D$. Then $q = ab = qcb$ implies that $1 = cb$, by the cancelation law in D, and hence b is a unit. If $< a >= D$ then $1 \in< a >$ shows that $1 = ad$ for some $d \in D$, and hence a is a unit. Thus q is an irreducible element. □

The above result is not true in a ring R which is not an integral domain.

Consider the ring $\mathbb{Z}_6$. Then $[1]$ and $[5]$ are the only units in $\mathbb{Z}_6$. Now $M = \{[0], [3]\} =< [3] >$ is a maximal ideal, but $[3] = [3][3]$ shows that $[3]$ is not an irreducible element of $\mathbb{Z}_6$.

Hence the converse of the above theorem is not true.

Example 0.7. *Consider the ring* $R = \mathbb{Z}[x]$*. Then* x *is an irreducible element of* R*. To prove this, consider* $f(x), g(x) \in \mathbb{Z}[x]$ *such that* $x = f(x)g(x)$*. Then* $1 = \deg f(x) + \deg g(x)$*, since* $\mathbb{Z}$ *is an integral domain, which implies that either* $\deg f(x) = 0$ *or* $\deg g(x) = 0$*. If* $\deg f(x) = 0$ *then* $f(x) = a \in \mathbb{Z}$*, and so* $x = ag(x)$ *which implies that* $1 = ab_1$ *for some* $b_1 \in \mathbb{Z}$*. Thus* $a = f(x)$ *is a unit in* $\mathbb{Z}[x]$*. Similarly, if* $\deg g(x) = 0$ *then* $g(x)$ *is a unit. Thus* x *is irreducible.*

But $\mathbb{Z}[x]/ < x > \simeq \mathbb{Z}$ *shows that* $< x >$ *is not a maximal ideal of* $\mathbb{Z}[x]$*, since* $\mathbb{Z}$ *is not a field.*

1 Summary

- Let R be a commutative ring with 1 and p be a nonzero nonunit element of R.

  (i) Then p is called irreducible if for every $a, b \in R$, $p = ab$ implies that either a or b is a unit.

  p is called reducible if p is not irreducible.

  (ii) Then p is called prime if for every $a, b \in R$, $p \mid ab$ implies that either $p \mid a$ or $p \mid b$.

- $2 + i\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$ is an irreducible element but not a prime.

- $[3] \in \mathbb{Z}_6$ is a prime element but not irreducible.

- In an integral domain every prime element is irreducible.

- Let R be a commutative ring with 1 and let $P =< p >$ be a nonzero ideal of R. Then P is a prime ideal if and only if p is a prime element.

- Let D be an integral domain. If $M =< q >$ is a nonzero maximal ideal of D then q is an irreducible element.

  The converse is not true.