

---

**Definition.** Let  $D$  be an integral domain, and let  $a, b, c \in D$ .

If  $a = ub$  for some unit  $u \in D$ , then  $a$  and  $b$  are *associates*.

If  $a$  is a nonzero non-unit, and writing  $a = bc$  implies  $b$  or  $c$  is a unit,  $a$  is *irreducible*.

If  $a$  is a nonzero non-unit, and  $a|bc$  implies  $a|b$  or  $a|c$ , then  $a$  is *prime*.

**Definition.** Let  $d \in \mathbb{Z}$  such that  $d \neq 1$  and  $d$  is not divisible by the square of a prime. Then  $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$  is a ring equipped with a norm function  $N$  with the properties described in Lemma A.

**Lemma A.** The norm function  $N : \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{N}$  defined by  $N(a + b\sqrt{d}) = |a^2 - db^2|$  satisfies:

- (1)  $N(x) = 0$  iff  $x = 0$ ,
  - (2)  $N(xy) = N(x)N(y)$  for all  $x, y$ ,
  - (3)  $x \in \mathbb{Z}[\sqrt{d}]$  is a unit iff  $N(x) = 1$ , and
  - (4) For  $x \in \mathbb{Z}[\sqrt{d}]$ , if  $N(x)$  is prime, then  $x$  is irreducible in  $\mathbb{Z}[\sqrt{d}]$ .
- 

(1) Prove Lemma A. Parts (1)-(2) are straightforward calculation. For part (3), recall the definition of a unit, and remember that  $N$  is a nonnegative integer function. Part (4) relies on parts (2)-(3).

---

**Theorem 18.1: Prime Implies Irreducible.**

In an integral domain, every prime is an irreducible.

**Theorem 18.2: PID Implies Irreducible Equals Prime.**

In a principle ideal domain, an element is an irreducible iff it is a prime.

**Lemma B.**  $\mathbb{Z}[x]$  is not a principal ideal domain.

---

- (2) Trace through example 1: in  $\mathbb{Z}[\sqrt{-3}]$ ,  $1 + \sqrt{-3}$  is irreducible but not prime.
- (a) Compute  $N(1 + \sqrt{-3})$ . Suppose that  $1 + \sqrt{-3}$  can be written as  $xy$  for some  $x, y \in \mathbb{Z}[\sqrt{-3}]$ . Use Lemma A(2) to write down the possibilities for  $N(x), N(y)$ . Assuming neither  $x$  nor  $y$  is a unit, what possibilities for  $N(x), N(y)$  remain?
- (b) Solve  $N(x) = 2$  for  $x$ , by writing  $x$  in the form  $a + b\sqrt{-3}$ . What is the conclusion?
- (c) Verify the equation  $(1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2$ , so that  $(1 + \sqrt{-3})$  divides  $2 \cdot 2$ .
- (d) If  $(1 + \sqrt{-3})$  is to be prime, then  $(1 + \sqrt{-3})|2 \cdot 2$  must imply that  $(1 + \sqrt{-3})|2$ ; in other words, there must be a solution to the equation  $(1 + \sqrt{-3})(a + b\sqrt{-3}) = 2$ . Try to solve this equation and draw a conclusion about whether  $(1 + \sqrt{-3})$  is prime.

- (3) Let  $a, b$  be elements of an integral domain. Prove that if  $b$  is nonzero, and  $a$  is not a unit, then  $\langle ab \rangle$  is a proper subset of  $\langle b \rangle$ .