Exercise 18.1. *Let $Z[\sqrt{d}] = \{ a + b\sqrt{d} \mid a\ b \in Z \}$, where where d is not 1 and is not divisible by the square of a prime (Note that d needs not to be positive). The norm of $a+b\sqrt{d} \in Z[\sqrt{d}]$ is given by $N(a+b\sqrt{d}) = |a^2 - db^2|$. Verify the following properties:*

1. *$N(x) = 0$ iff $x = 0$*
2. *$N(xy) = N(x)N(y)$*
3. *$N(x) = 1$ iff x is a unit*
4. *$N(x)$ is prime implies x is irreducible over $Z[\sqrt{d}]$*

Proof.

1. If $N(x) = 0$, then $a^2 = db^2$, however, d is not divisible by the square of any prime and a^2 is a product of some squares of prime, therefore $a = b = 0$.
2. Trivial.
3. If $N(a+b\sqrt{d}) = 1$, then $(a+b\sqrt{d})(a-b\sqrt{d}) = \pm 1$. If $a+b\sqrt{d}$ is a unit, then $N(1) = N((a+b\sqrt{d})(s+t\sqrt{d})) = 1$, by property 2, we know $N(a+b\sqrt{d})N(s+t\sqrt{d}) = 1$, which implies $N(a+b\sqrt{d}) = N(s+t\sqrt{d}) = 1$.
4. Suppose $x = ab$, then $N(x) = N(ab) = N(a)N(b)$. We know one of $N(a)$ and $N(b)$ is 1 since $N(x)$ is prime, which implies one of a and b is unit, therefore x is irreducible.

□

Exercise 18.2. *In an integral domain, show that a and b are associates iff $\langle a \rangle = \langle b \rangle$.*

Proof.

- ($\Rightarrow$) If $a = cb$, then $b \in \langle a \rangle$. Similarly, $c^{-1}a = b$, therefore $a \in \langle b \rangle$.
- ($\Leftarrow$) If $\langle a \rangle = \langle b \rangle$, then $b \in \langle a \rangle$, which implies $b = ac$ for some c. Similarly, $a \in \langle b \rangle$, then $a = bd$ for some d.

□

Exercise 18.3. *Show that the union of a chain $I_0 \subset I_1 \subset \dots$ of ideals of a ring R is an ideal of ring R.*

Proof. Let $I = I_0 \cup I_1 \cup \dots$, for any $a \in I$, a must belongs to some I_i, then for any $b \in R$, we know $ab \in I_i$ since I_i is an ideal, therefore $ab \in I$ since $I_i \subseteq I$. $\square$

Exercise 18.4. *In an integral domain, let r an irreducible and a a unit, show that ar is an irreducible.*

Proof. Let D an integral domain, suppose $ar = st$ for some $s\ t \in D$, then $r = a^{-1}st$. Then we know one of $a^{-1}s$ and t is a unit since r is irreducible. If $a^{-1}s$ is a unit, so is s; if t is a unit, so is t. $\square$

Exercise 18.5. *Let D an integral domain and $a\ b \in D$ where $b \neq 0$. Show that $\langle ab \rangle \subset \langle b \rangle$ iff a is not a unit.*

Proof.

- ($\Rightarrow$) If a is a unit, then $b = a^{-1}ab$, which implies $\langle b \rangle \subseteq \langle ab \rangle$.
- ($\Leftarrow$) If $\langle ab \rangle = \langle b \rangle$, then $b \in \langle ab \rangle$ and $b = cab$ for some $c \in D$. Then $1 = ca$ by cancellation, which means a is a unit with an inverse c.

$\square$

Exercise 18.6. *Let D be an integral domain. Define $a \sim b$ iff a and b are associates. Show that is an equivalence relation on D.*

Proof.

- (Reflexivity) $a \sim a$ by $a = 1a$.
- (Symmetry) If $a \sim b$, then $a = cb$ where c is a unit, then $b = c^{-1}a$, therefore $b \sim a$.
- (Transitivity) If $a \sim b$ and $b \sim c$, then $a = sb$ and $b = tc$, then $a = stc$, therefore $a \sim c$.

$\square$

Exercise 18.8. *Let D be an Euclidean domain with measure d. Prove that $u \in D$ is a unit iff $d(u) = d(1)$.*

Proof. By $d(u) \leq d(uu^{-1}) = d(1)$ (The 1st property of Euclidean domain) and $d(1) \leq d(1u) = d(u)$, we know $d(u) = d(1)$. $\square$

Exercise 18.9. *Let D be an Euclidean domain with measure d. Prove that if a and b are associates in D, then $d(a) = d(b)$.*

Proof. We know $a = cb$, then $d(a) \leq d(c^{-1}a) = d(b)$ and $d(b) \leq d(cb) = d(a)$, therefore $d(a) = d(b)$. $\square$

Exercise 18.10. *Let D be a principal ideal domain and let $p \in D$. Prove that $\langle p \rangle$ is a maximal ideal in D iff p is irreducible.*

Proof.

- ($\Rightarrow$) If $\langle p \rangle$ is maximal, then it is also prime, therefore p is prime, then p is irreducible by Theorem 18.1.
- ($\Leftarrow$) If p is irreducible, suppose I an ideal that $I \supseteq \langle p \rangle$. Since D is a principal ideal domain, we know $I = \langle q \rangle$ for some $q \in D$. Then $p = qr$ since $p \in \langle q \rangle$, therefore one of q and r is unit.
  - If q is unit, then $I = D$.
  - If r is unit, then $q = r^{-1}p$, therefore $\langle p \rangle = \langle q \rangle = I$.

  Therefore $\langle p \rangle$ is a maximal ideal in D.

$\square$

Exercise 18.11. *Let d be an integer such that $d < 1$ and it is not divisible by the square of a prime. Prove that the only units of $Z[\sqrt{d}]$ are $+1$ and -1.*

Proof. Let $a + b\sqrt{d} \in Z[\sqrt{d}]$ a unit, then $N(a + b\sqrt{d}) = |a^2 - b^2 d| = 1$. Note that $d < 1$, therefore $-b^2 d \geq 0$, which means $a^2 - b^2 d = 1$.

- If $a = 0$, then $-b^2 d = 1$. We know $b^2 < 1$ by $-d > 1$, which implies $b = 0$, but now $a = b = 0$, and $0 + 0\sqrt{d}$ cannot be a unit.
- If $a \neq 0$, then $a^2 > 0$, which means $-b^2 d \leq 0$. But we know $-b^2 d \geq 0$, therefore $-b^2 d = 0$ and then $b = 0$, $a^2 = 1$. We can conclude that $a = \pm 1$.

$\square$

Exercise 18.12. *Let D be a principal ideal domain. Show that every proper ideal of D is contained in a maximal ideal of D.*

Proof. Let I a proper ideal of D. If there is no any ideal D that properly contains I, then I is a maximal ideal. Let J an proper ideal that properly contains I, if J is not a maximal ideal, then find a maximal ideal that containing J. This algorithm must stop, otherwise it implies an infinite strictly increasing chain $I \subset J \subset \dots$, which makes nonsense by Lemma 18.1. $\square$

Exercise 18.14. *Show that $1 - i$ is irreducible in $Z[i]$.*

Proof. Define the norm of $a + bi$ by $N(a + bi) = a^2 + b^2$, then:

- $N((a+bi)(c+di)) = N((ac-bd)+(ad+bc)i) = (ac-bd)^2+(ad+bc)^2 = (ac)^2-2abcd+(bd)^2+(ad)^2+2abcd+(bc)^2 = (ac)^2+(bd)^2+(ad)^2+(bc)^2 = (a^2 + b^2)c^2 + (a^2 + b^2)d^2 = (a^2 + b^2)(c^2 + d^2) = N(a + bi)N(c + di)$.
- If $N(a + bi) = a^2 + b^2 = 1$, we know a^2 and b^2 are nonzero integer, therefore either $a^2 = 1$ or $b^2 = 1$, which means $a + bi$ is one of these: ± 1 and $\pm i$, therefore $a + bi$ is a unit.
- Suppose $1 - i = ab$, then $2 = (1 + 1) = N(1 - i) = N(ab) = N(a)N(b)$. Since 2 is a prime, then either $N(a) = 2$ or $N(b) = 2$, which implies either $N(b) = 1$ or $N(a) = 1$, therefore $1 - i$ is irreducible.

$\square$

Exercise 18.19. *Let $p \in Z$ a prime such that $p = a^2 + b^2$ where $a, b \in Z$. Prove that $a + bi$ is irreducible in $Z[i]$.*

Proof. According to Exercise 18.14, we know $N(a + bi) = a^2 + b^2 = p$ is a prime, therefore $a + bi$ is irreducible.

For example, 5 and $1 + 2i$ (or $2 + 1i$), 2 and $1 + i$, 17 and $1 + 4i$. $\square$

Exercise 18.20. *Prove that $Z[\sqrt{-3}]$ is not a PID.*

Proof. Consider $4 \in Z[\sqrt{-3}]$, it is easy to see that $2 * 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Therefore $Z[\sqrt{-3}]$ is not a UFD, then it is not a PID. $\square$

Exercise 18.24. *Let F a field, prove that any non-zero prime ideal in $F[x]$ is also a maximal ideal.*

Proof. We know $F[x]$ is a principal ideal domain, therefore any prime ideal in $F[x]$ has form $\langle p \rangle$ and p is a prime. Then p is an irreducible, finally $\langle p \rangle$ is maximal by Exercise 18.10. $\square$

Exercise 18.37. *An ideal A of a commutative ring R with unity is said to be finitely generated if there exist elements $a_0, a_1, \cdots, a_n \in A$ such that $A = \langle a_0, a_1, \cdots, a_n \rangle$.*

An integral domain R is said to satisfy the ascending chain condition if every strictly increasing chain of ideals $I_0 \subset I_1 \subset \dots$ has a finite length.

Show that an integral domain R satifies the ascending chain condition iff every ideal of R is finitely generated. Note that this is the generialized version of Lemma 18.1, finitely generate instead of principal ideal.

Proof. $\square$