1. Let H, I, J be nonzero ideals in dedekind domain D. Given $HI = HJ$, prove $I = J$.

Proof We show $I \subseteq J$. Then, by symmetry, $J \subseteq I$, which shows $I = J$.

We know that any ideal in a dedekind domain has an inverse ideal. The ideal H has some ideal H' such that $H'H = \langle \alpha \rangle$ for some nonzero element $\alpha \in H$. Write:

$$H'HI = H'HJ \quad \text{or} \quad \langle \alpha \rangle I = \langle \alpha \rangle J$$

For any element $i \in I$, we extract $\alpha i = \alpha j$ for some $j \in J$. D is a domain, so by cancellation, $i = j$. We conclude $I \subseteq J$ and thus $I = J$. □

2. Let $R := \mathbb{Z}[\sqrt{-3}]$. Also, define an ideal in R, $I = \langle 2, 1 + \sqrt{-3} \rangle$.

- Prove $I \neq \langle 2 \rangle$
- Prove $I^2 = \langle 2 \rangle I$
- Is R a dedekind domain?

Solution We start with showing that I is not equal to the principal ideal generated by 2. Assume for a contradiction, that indeed $I = \langle 2 \rangle$. Then, it must be $1 + \sqrt{-3} \in \langle 2 \rangle$. There must be some element $r \in R$ such that:

$$2r = 1 + \sqrt{-3} \quad \text{or} \quad r = \frac{1 + \sqrt{-3}}{2}$$

by expanding our search to the field of quotients. However, $r \notin Z[\sqrt{-3}]$, for the field of quotients is indeed a field, and inverses are unique. We reach a contradiction and $I \neq \langle 2 \rangle$

□

We move on to show $I^2 = \langle 2 \rangle I$. By ideal algebra:

$$\langle 2, 1 + \sqrt{-3}^2 \rangle = \langle 4, 2 + 2\sqrt{-3}, (1 + \sqrt{-3})^2 \rangle$$

$$\langle 4, 2 + 2\sqrt{-3}, -2 + 2\sqrt{-3} \rangle = \langle 2 \rangle \langle 2, 1 + \sqrt{-3}, -1 + \sqrt{-3} \rangle$$

Notice that $-1 + \sqrt{-3} = 1 + \sqrt{-3} - 2$. Thus, we conclude:

$$I^2 = \langle 2 \rangle \langle 2, 1 + \sqrt{-3} \rangle = \langle 2 \rangle I$$

as desired. □

Sadly, R is not a dedekind domain. In a dedekind domain, ideals cancel out. Thus $I^2 = \langle 2 \rangle I$ implies $I = \langle 2 \rangle$, which we have proven to be false on the first part. ↯

□

3. Prove that $\langle 3, 1 \pm \sqrt{-5}\rangle$ are prime ideals in the ring $\mathbb{Z}[\sqrt{-5}]$

Proof Denote $I := \langle 3, 1+\sqrt{-5}\rangle$ Consider the following line of Ideal algebra:

$$\langle 3, 1+\sqrt{-5}\rangle^2 = \langle 9, 3+3\sqrt{-5}, -4+2\sqrt{-5}\rangle$$

We can add a ring multiple of one entry and add to another generator and still get the same ideal. Thus:

$$= \langle 9, 3+3\sqrt{-5}+4-2\sqrt{-5}, -4+2\sqrt{-5}\rangle = \langle 9, 7+\sqrt{-5}, -4+2\sqrt{-5}\rangle$$

$$= \langle 9, 7+\sqrt{-5}, -4+2\sqrt{-5}-14-2\sqrt{-5}\rangle = \langle 9, 7+\sqrt{-5}, -18\rangle$$
$$= \langle 9, 7+\sqrt{-5}\rangle = \langle 9, -2+\sqrt{-5}\rangle = \langle -2+\sqrt{-5}\rangle = \langle 2-\sqrt{-5}\rangle$$

In fact, this ideal is a prime ideal. This is because the element $2-\sqrt{-5}$ is prime in the ring $\mathbb{Z}[-5]$. According to the textbook, $\mathbb{Z}[\sqrt{-5}]$ is indeed a UFD, so it suffices to show that $2-\sqrt{-5}$ is irreducible. The element has a norm of 9. Assuming that this element has a nonunit divisor, the norm of the divisor must necessarily be 3.

Assume, for some $(a+b\sqrt{-5})|(2-\sqrt{-5})$:

$$N(a+b\sqrt{-5}) = 3 \quad \text{and} \quad a^2+5b^2 = 3$$

Clearly, there are no integer solutions for a, b. Hence the element is irreducible, and the principal ideal generated by it is also prime. I^2 must be prime, but then, $I|I^2$. This means, by ideal cancellation, $I = R$. (Ideal cancellation is justified for $\mathbb{Z}[\sqrt{-5}]$ is a ring of integers, and all ring of integers are dedekind domains).

We derive a contradiction by demonstrating that I^2 is proper. If $I = R$, $I^2 = R = \langle 1\rangle$. Thus, $1 \in \langle 2-\sqrt{-5}\rangle$, so the multiplicative inverse of $2-\sqrt{-5}$ must be in the ring R. Again, in the ring of quotients,

$$\frac{1}{2-\sqrt{-5}} = \frac{2+\sqrt{-5}}{9}$$

and the latter element is clearly not in the ring $\mathbb{Z}[\sqrt{-5}]$ ↯

For the ideal $I' := \langle 3, 1-\sqrt{-5}\rangle$, it suffices to show that I'^2 is principal of a nonunit element. We can then repeat the argument above. The following lines of algebra concludes the proof:

$$\langle 3, 1-\sqrt{-5}\rangle^2 = \langle 9, 3-3\sqrt{-5}, -4-2\sqrt{-5}\rangle$$
$$= \langle 9, 3-3\sqrt{-5}+4+2\sqrt{-5}, -4-2\sqrt{-5}\rangle = \langle 9, 7-\sqrt{-5}, -4-2\sqrt{-5}\rangle$$

$$= \langle 9, 7-\sqrt{-5}, -4-2\sqrt{-5}-14+2\sqrt{-5}\rangle = \langle 9, 7-\sqrt{-5}, -18\rangle$$
$$= \langle 9, 7-\sqrt{-5}\rangle = \langle 9, -2-\sqrt{-5}\rangle = \langle 2+\sqrt{-5}\rangle$$

$\square$

4. Let $K := Q(\sqrt{d})$ be a quadratic field where d is squarefree. Suppose $\mathcal{O}_K$ is a UFD. Prove the following:

- Let p be a prime in $\mathbb{Z}$ where $p|d$. Prove that p is an associate of a square of some prime element in $\mathcal{O}_K$

Q1 We first show that p is not prime, and hence must be reducible. Since p divides d, we can write:

$$(\sqrt{d})^2 = pa$$

for some integer a. Notice that $p \nmid \sqrt{d}$. Otherwise, we can write $\sqrt{d} = p\alpha$ for some $\alpha \in \mathcal{O}_K$. Again, in the field of quotients, $\alpha = \sqrt{d}/p$, but this element cannot be in the ring of integers unless $p = 2$. Moreover, even if $p = 2$, the ring of integers include only the element where the parity of the integer part and the irrational part match. Thus, $\sqrt{d}$ is always irreducible.

This factorization sees witness to the fact that p is nonprime. p must be reducible in O_K. We write:

$$p = \alpha\beta$$

For some $\alpha, \beta \in \mathcal{O}_K$ that is not a unit. Taking the norm, we observe that $N(\alpha) = p$ necessarilly. Otherwise, one of the two elements will be a unit. From the norm statement, we deduce:

$$\alpha\bar{\alpha} = p$$

Consider the case $d \not\equiv 1(mod\, 4)$. Write out $\alpha = a + b\sqrt{d}$ for some integer a, b. We obtain $a^2 - b^2 d = p$. $p|d$ so $p|a^2$ and $p|a$. For α has a prime norm, it is an irreducible. We will show that p is an associate of α^2.

$$\frac{\alpha^2}{p} = \frac{(a + b\sqrt{d})^2}{p} = \frac{a^2 + b^2 d + 2ab\sqrt{d}}{p}$$

$p|a, d$ guarantees that the fraction above is indeed in the ring of integers. Finally, we take the norm of this integer to demonstrate that it is indeed a unit:

$$N(\alpha^2/p) = \left(\frac{a^2 + b^2 d}{p}\right)^2 - 4a^2b^2d/p^2$$

$$= \frac{(a^2 - b^2 d)^2}{p^2} = p^2/p^2 = 1$$

which condludes the proof.

Consider the case $d \equiv 1(mod\, 4)$. Write out $\alpha = (a + b\sqrt{d})/2$ for some integer a, b. We obtain $a^2 - b^2 d = 4p$. $p|d$ so $p|a^2$ and $p|a$. For α has a prime norm, it is an irreducible. We will show that p is an associate of α^2.

$$\frac{\alpha^2}{p} = \frac{(a+b\sqrt{d})^2}{4p} = \frac{a^2+b^2d+2ab\sqrt{d}}{4p}$$

$p|a, d$ guarantees that the fraction above is indeed in the ring of integers. Finally, we take the norm of this integer to demonstrate that it is indeed a unit:

$$N(\alpha^2/p) = \left(\frac{a^2+b^2d}{4p}\right)^2 - a^2b^2d/(4p^2)$$

$$= \frac{(a^2-b^2d)^2/16}{p^2} = p^2/p^2 = 1$$

which condludes the proof. $\square$

- Let p be an odd prime and d a square mod p. p is a multiple of two distinct primes.

Q2 Write $d = r^2(mod\, p)$ where r is some nonzero positive integer less than p. For p is an odd integer, we have $gcd(2r, p) = 1$. By Bezout's identity, extract integers n, m that satisfies:

$$2rn + pm = 1$$

Factorize the prime ideal generated by the prime p. Consider:

$$\langle p, \sqrt{d} + r\rangle\langle p, \sqrt{d} - r\rangle = \langle p^2, p(\sqrt{d} + r), p(\sqrt{d} - r), d - r^2\rangle$$

By the condition on d, $(d - r^2)/p$ must be an integer. Write:

$$\langle p\rangle\langle p, \sqrt{d} + r, \sqrt{d} - r, (d - r^2)/p\rangle = \langle p\rangle\langle p, 2r, \sqrt{d} + r, (d - r^2)/p\rangle$$

By Bezout's identity, it is possible to obtain a unit from a $\mathbb{Z}$ combination of p and $2r$. The latter ideal simplifies to the whole ring. Thus:

$$\langle p, \sqrt{d} + r\rangle\langle p, \sqrt{d} - r\rangle = \langle p\rangle$$

Still, it remains to show that the two ideals involved in this factorization are both proper. Assume for a contradiction that the right ideal is indeed the whole ring. Consequently:

$$\langle p, \sqrt{d} + r\rangle = \langle p\rangle \quad \text{and} \quad \sqrt{d} + r \in \langle p\rangle$$

There must exist some element $\alpha \in \mathcal{O}_K$ that satisfies:

$$p\alpha = \sqrt{d} + r$$

Observing this equation in the factor ring:

$$\alpha = \frac{\sqrt{d} + r}{p}$$

Clearly, this element is not in the ring of integers. A similar argument applies to the other ideal.

Since $\mathcal{O}_K$ is known to be a UFD, it is a PID. The two generators of the ideals $\langle p, \sqrt{d} + r\rangle\langle p, \sqrt{d} - r\rangle$ are both non-units. The product of the generators must be p. Hence, p reducible.

$$p = \alpha\beta$$

For some $\alpha, \beta \in \mathcal{O}_K$ that is not a unit. Taking the norm, we observe that $N(\alpha) = p$ necessarilly. Otherwise, one of the two elements will be a unit.

Start with $d \not\equiv 1(mod\, 4)$. From the norm statement, we deduce:

$$\alpha\bar{\alpha} = p \quad \text{and} \quad a^2 - db^2 = p$$

where $\alpha = a + b\sqrt{d}$.

It suffices to show that $\alpha, \bar{\alpha}$ are not associates of each other. We extend our search to the field of quotients. If the two elements are associates, $\alpha/\bar{\alpha}$ must yield a unit in the ring. However computation shows that this element is not even in the ring:

$$\frac{\alpha}{\bar{\alpha}} = \frac{a+b\sqrt{d}}{a-b\sqrt{d}} = \frac{a+b\sqrt{d}}{a-b\sqrt{d}}\frac{a+b\sqrt{d}}{a+b\sqrt{d}} = \frac{a^2+b^2d+2ab\sqrt{d}}{a^2-b^2d}$$

$$= 1 + \frac{2b^2d+2ab\sqrt{d}}{a^2-b^2d} = 1 + \frac{2b^2d+2ab\sqrt{d}}{p}$$

For this element to be in the ring of integers, $p|2b^2d$ by looking at the rational part (this is in $\mathbb{Z}$). This implies $p|b$, but then, $p|a$. Recall:

$$a^2 - db^2 = p$$

By dividing both sides by p, we obtain, $p|1$, a contradiction. $\lightning$

We can repeat the process for $p \equiv 1(mod\ 4)$. The division relation is mostly exploited for odd p, and it is not hard to deduce a contradiction using a similar argument. $\square$

- If p is an odd prime, and d is not a square of mod p, it is guaranteed that p is prime in the ring $\mathcal{O}_K$.

Q3 Start with the case $k \not\equiv (mod\ 4)$. Assume p to be reducible. Repeating the norm argument, we derive some element $\alpha \in \mathcal{O}_K$ such that $N(\alpha) = p$. Expand $\alpha := a + b\sqrt{d}$ for integers a, b. Write:

$$a^2 - b^2 d = p$$

We claim $p \nmid b$. Otherwise, $p|a$ and dividing out p,

$$p(a/p)^2 - p(b/p)^2 d = 1$$

which in turn implies $p|1$, a contradiction.

p is an odd prime. Hence, in $\mathbb{Z}$, $gcd(p, b) = 1$. There is a modular inverse of b in mod p. In other words, there exists $b' \in \mathbb{Z}$ such that $bb' \equiv = 1(mod\ p)$.

Reconsider the norm equation in mod p.

$$a^2 - b^2 d \equiv 0(mod\ p)$$

$$a^2 \equiv b^2 d(mod\ p)$$

$$(ab')^2 \equiv (bb')^2 d \equiv d(mod\ p)$$

Oh, but d cannot be a square mod p. We have reached a contradiction. $\lightning$Now let $k \equiv (mod\ 4)$. Assume p to be reducible. Repeating the norm argument, we derive some element $\alpha \in \mathcal{O}_K$ such that $N(\alpha) = p$. Expand $\alpha := a + b\sqrt{d}$ for integers a, b. Write:

$$(a^2 - b^2 d)/2 = p \quad \text{or} \quad a^2 - b^2 d = 2p$$

We claim $p \nmid b$. Otherwise, $p|a$ and dividing out p,

$$p(a/p)^2 - p(b/p)^2 d = 2$$

which in turn implies $p|2$, a contradiction.

p is an odd prime. Hence, in $\mathbb{Z}$, $gcd(p, b) = 1$. There is a modular inverse of b in mod p. In other words, there exists $b' \in \mathbb{Z}$ such that $bb' \equiv = 1(mod\ p)$.

Reconsider the norm equation in mod p.

$$a^2 - b^2 d \equiv 0(mod\ p)$$

$$a^2 \equiv b^2 d(mod\ p)$$

$$(ab')^2 \equiv (bb')^2 d \equiv d(mod\ p)$$

Oh, but d cannot be a square mod p. We have reached a contradiction. $\square$

Q4

Solution

Consider this product of ideals:

$$\langle 2p, \sqrt{d}+1\rangle\langle 2p, \sqrt{d}-1\rangle$$

$$= \langle 4p^2, 2p\sqrt{d}+2p, 2p\sqrt{d}-2p, d-1\rangle$$
$$= \langle 4p^2, 4p, 2p\sqrt{d}-2p, d-1\rangle$$
$$= \langle 4p, 2p\sqrt{d}-2p, d-1\rangle$$

Notice that since d is odd, $d-1$ must be even. Write:

$$= \langle 2\rangle\langle 2p, p\sqrt{d}-p, (d-1)/2\rangle$$

If $d \equiv 3(mod\, 4)$, then $(d-1)/2$ is odd. In fact, this implies $gcd(2p, (d-1)/2) = 1$ and by Bezout's identity, it is possible to extract a $\mathbb{Z}$ combination of the two elements that result in a unit. The right ideal collapses to the entire ring. So we write:

$$\langle 2p, \sqrt{d}+1\rangle\langle 2p, \sqrt{d}-1\rangle = \langle 2\rangle$$

Now we show that the two ideals involved in the product are both proper. Assume for a contradiction that the left ideal, $\langle 2p, \sqrt{d}+1\rangle$ is the whole ring. Then, $\langle 2p, \sqrt{d}-1\rangle = \langle 2\rangle$ so $2 \in \langle 2p, \sqrt{d}-1\rangle$. In turn, $\langle 2p, \sqrt{d}-1\rangle = \langle 2p, \sqrt{d}+1\rangle$ and both ideals are the entire ring. The product, $\langle 2\rangle$ must be the whole ring, but this is not true, for the element $1/2$ in the fractional field is not included in the entire ring. Both ideals are proper.

Repeat the argument used on Q2. $\mathcal{O}_K$ is a UFD and hence is a PID. $\langle a\rangle\langle b\rangle = \langle p\rangle$ for some principal ideals that corresponds to $\langle 2p, \sqrt{d}+1\rangle, \langle 2p, \sqrt{d}-1\rangle$. $ab = p$ for nonunit a, b and p is reducible.

Consider the case $d \equiv 1(mod\, 4)$. Rewrite:

$$= \langle 2\rangle\langle 2p, p\sqrt{d}-p, (d-1)/2\rangle$$

This time, $(d-1)/2$ is even, and thus, $gcd(2p, (d-1)/2) = 2$. The ideal collapses to:

$$= \langle 2\rangle\langle 2, p\sqrt{d}-p\rangle$$

And for p is odd:

- Let $2 \nmid d$. When is 2 a prime, square of a prime, or a product of two primes?

Claim 1 If $d \equiv 5(mod\, 8)$ then 2 is prime.

Proof We assume for a contradiction that there is some d where 2 is reducible. Again, by the norm argument, we obtain an element $\alpha \in \mathcal{O}_K$ where $N(\alpha) = 2$. $d \equiv (mod\, 4)$ so write $\alpha = \frac{a+b\sqrt{d}}{2}$ for some integer a, b. Taking the norm:

$$N(\alpha) = \frac{a^2 - b^2 d}{4} = 2$$

$$a^2 - b^2 d = 8$$

It is convinient to remember that the quadratic residue of 8 is $0, 1, 4$. Taking mod 5 of the equation:

$$a^2 - 5b^2 \equiv 0(mod\, 8) \quad \text{and} \quad a^2 \equiv 5b^2(mod\, 8)$$

Trying all the slurs of possibilities for the residue of b^2, we claim $a^2 \equiv b^2 \equiv 0(mod\, 8)$. This in turn implies that a, b are multiples of 4. Back to the original equation:

$$16(a/4)^2 - 16(b/4)^2 d = 8 \quad \text{and} \quad 2(a/4)^2 - 2(b/4)^2 d = 1$$

The equation implies $2|1$, a contradiction. ↯ $\square$

Book 5.8 Let $\mathfrak{p}, \mathfrak{q}$ be distinct prime ideals in a dedekind domain $\mathcal{O}_K$. Prove that $\mathfrak{p} + \mathfrak{q} = \mathcal{O}_K$ and $\mathfrak{p}\mathfrak{q} = \mathfrak{p} \cap \mathfrak{q}$.

Proof Start with the first statement. Assume for a contradiction that $\mathfrak{p} + \mathfrak{q}$ is a proper ideal. All proper ideals are contained in a maximal ideal. Let M be the maximal ideal containing the sum of the two prime ideals. M is maximal, hence prime.

$\mathfrak{p}, \mathfrak{q} \subseteq \mathfrak{p} + \mathfrak{q} \subseteq M$, so $M | \mathfrak{p}, \mathfrak{q}$. Since $\mathfrak{p}$ and $\mathfrak{q}$ is a prime ideal, and since the factorization of ideals are unique, $M = \mathfrak{p} = \mathfrak{q}$. This contradicts the fact that the two prime ideals are unique. ✓.

Now, show the second statement. Denote the intersect of the two ideals as I. By construction, I is included in both $\mathfrak{p}, \mathfrak{q}$. These two ideals contain I. Hence, $\mathfrak{p}|I$ and $\mathfrak{q}|I$. Again, ideals factor uniquely in dedekind domains and $\mathcal{O}_K$ is a dedekind domain. Ergo, $\mathfrak{p}\mathfrak{q}|I$ and we deduce $\mathfrak{p}\mathfrak{q} \supseteq I$.

By strong closure of ideals, $\mathfrak{p}\mathfrak{q} \subseteq \mathfrak{p}$. Write any element in the product ideal as:

$$\alpha = \sum_{i=1}^{N} p_i q_i$$

where each p_i, q_i are elements of $\mathfrak{p}$ and $\mathfrak{q}$ for all $1 \leq i \leq N$. Each summand is in $\mathfrak{p}$, and the closure of $\mathfrak{p}$ under addition guarantees $\alpha \in \mathfrak{p}\mathfrak{q}$.

By symmetry, $\mathfrak{p}\mathfrak{q} \subseteq \mathfrak{q}$. Thus, $\mathfrak{p}\mathfrak{q} \subseteq \mathfrak{p} \cap \mathfrak{q} = I$ We have shown containment both ways. $\mathfrak{p}\mathfrak{q} = \mathfrak{p} \cap \mathfrak{q}$

□

Book 5.12 In the ring $\mathbb{Z}[\sqrt{-5}]$, find all the ideals that contain the element 6.

Proposition In the ring $\mathbb{Z}[\sqrt{-5}]$, elements with norm 4, 6, 9 are irreducible.

Proof If such an element is not prime, there must exist a nonunit divisor that has a norm of 2 or 3. Assume there exists some ring element $\alpha = a + b\sqrt{-5}$ that has a norm of 2 or 3. It must be:

$$a^2 + b^2 = 2 \quad \text{or} \quad a^2 + b^2 = 3$$

Both equations have no integer solutions. □

Proposition The only factorization of 6 in the ring $\mathbb{Z}[\sqrt{-5}]$ is:

$$6 = 2 \cdot 3 \quad \text{or} \quad 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Proof Compute $N(6) = 36$. The possible nonunit divisors of 36 are:

$$n = 2, 3, 4, 6, 9, 12, 18, 36$$

Let n be the norm of some divisor of 6. We can eliminate $n = 2, 3$ for no element can have such a norm in the ring $\mathbb{Z}[\sqrt{-5}]$. For $n \geq 6$, the symmetry will guarantee that the norm of the other divisor will fall into the values of n that are less than 6.

We are left with:

$$n = 4, 6$$

$n = 4$ implies that the element in question is exclusively 2. $n = 6$ implies the element is one of $1 \pm \sqrt{-5}$ By the first proposition, these elements along with their corresponding 6-conjugates are also irreducible. $\square$

Corollary 1 The divisors of 6 in $\mathbb{Z}[\sqrt{-5}]$ are:

$$\{2, 3, 1 \pm \sqrt{-5}\}$$

Corollary 2 The ideals in $\mathbb{Z}[\sqrt{-5}]$ are those which contain $\{2, 3, 1 \pm \sqrt{-5}\}$ in its generators.

Proof $\mathbb{Z}[\sqrt{-5}]$ is the ring of integers of the quadratic field where $d = -5 \equiv 3(mod\ 4)$. The ring of integers of any number fields are noetherian, and thus all ideals are finitely generated. It is trivial to see that if one of the generators in the ideal is the divisor of 6, the ideal contains 6. $\square$

Example Some(but not all) Ideals of $\mathbb{Z}[\sqrt{-5}]$ that include 6

$$\langle 2 \rangle, \langle 3 \rangle, \langle 2, 1 + \sqrt{-5} \rangle, \langle 2, \sqrt{-5} \rangle$$

and the list goes on.