1. Prove that $I := \langle 2, 1+\sqrt{-5}\rangle$ is not principal in the ring $\mathbb{Z}[\sqrt{-5}]$

Proof First, we claim that $\{2, 1+\sqrt{-5}\}$ is indeed an integral base of ideal I. Take any element from ideal I and write:

$$\begin{aligned} &2(a+b\sqrt{-5}) + (1+\sqrt{-5})(c+d\sqrt{-5}) \\ &= 2a + 2b\sqrt{-5} + c - 5d + (c+d)\sqrt{-5} \\ &= (1+\sqrt{-5})(2b+c+d) - 2b - c - d + 2a + c - 5d \\ &= (1+\sqrt{-5})(2b+c+d) + 2a - 2b - 6d \\ &= (1+\sqrt{-5})(2b+c+d) + 2(a-b-3d) \end{aligned}$$

where a, b, c, d are integers. We have successfully expressed an arbitrary element in I as a $\mathbb{Z}$-combination of the base.

Indeed the combination is unique. Assume for a contradiction that two $\mathbb{Z}$ combinations of the base are equal to each other. Write, for some integers $a, \bar{a}, b, \bar{b}$:

$$a + (1+\sqrt{-5})b = \bar{a} + (1+\sqrt{-5})\bar{b}$$

Comparing the coefficients of $\sqrt{-5}$, we realize $b = \bar{b}$ and hence $a = \bar{a}$ which contradicts our assumption that the two combinations are distinct. ↯

Now that we have obtained the $\mathbb{Z}$ basis of I, it is possible to compute the norm of I. Recall:

$$N(I) = \sqrt{\left|\frac{\Delta[a_1, a_2, \ldots, a_n]}{\Delta}\right|}$$

where Δ denotes the discriminant of the ring, and $\Delta[a_1, a_2, \ldots, a_n]$ denotes the discriminant of the $\mathbb{Z}$-basis of I.

Write:

$$\Delta = \left|\begin{vmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{vmatrix}^2\right| = |(2\sqrt{-5})^2| = 20$$

Moreover:

$$\Delta[I] = \left|\begin{vmatrix} 2 & 1+\sqrt{-5} \\ 2 & 1-\sqrt{-5} \end{vmatrix}^2\right| = |(4\sqrt{-5})^2| = 80$$

Thus:

$$N(I) = \sqrt{80/20} = 2$$

Assume for a contradiction that I is a principal ideal. The generator of I must have the same element-wise norm as the norm of I. However, all nonzero elements of the ring $\mathbb{Z}[\sqrt{-5}]$ has a norm greator than 5: it is impossible for an element to have a norm of $N(I) = 2$. We reach a contradiction and conclude that I is not principal. □

2. In the ring $\mathbb{Z}[\sqrt{-5}]$, ideal I is defined as $I := \langle 7, 3+\sqrt{-5}\rangle$. Show that I is not principal but I^2 is principal. Conclude that I has an order of 2 in the class group.

Proof In fact, $I^2 = \mathbb{Z}[\sqrt{-5}]$. To see this, consider the following lines of ideal algebra:

$$\begin{aligned} I^2 &= \langle 7, 3+\sqrt{-5}\rangle^2 \\ &= \langle 49, 9-5+6\sqrt{-5}, 21+7\sqrt{-5}\rangle \\ &= \langle 49, 4+6\sqrt{-5}, 21+7\sqrt{-5}\rangle \\ &= \langle 49, 4+\sqrt{-5}, 17+\sqrt{-5}\rangle \\ &= \langle 49, -108, 17+\sqrt{-5}\rangle \\ &= \langle 49, -10, 17+\sqrt{-5}\rangle \\ &= \langle -1, -10, 17+\sqrt{-5}\rangle = \langle -1\rangle = \mathbb{Z}[\sqrt{-5}] \end{aligned}$$

So $I^2 = \mathbb{Z}[\sqrt{-5}]$ as desired ✓

Move on to show that ideal I is not principal. Like the previous problem, we will find the $\mathbb{Z}$ basis for I, and compute the norm of I. We purport that the $\mathbb{Z}$-basis of I is $\{7, 3+\sqrt{-5}\}$.

It is evident that:

$$Span_{\mathbb{Z}}\{7, 3+\sqrt{-5}\} \subseteq I$$

We wish to show the inclusion the other way, i.e:

$$I \subseteq Span_{\mathbb{Z}}\{7, 3+\sqrt{-5}\}$$

Take any element $\alpha \in I$. Express it as:

$$\alpha := (a+\sqrt{-5})7 + (\bar{a}+\bar{b}\sqrt{-5})(3+\sqrt{-5})$$

where $a, \bar{a}, b, \bar{b} \in \mathbb{Z}$. We wish to show that it is possible to express α as a $\mathbb{Z}$-combination of our claimed basis set, $\{7, 3+\sqrt{-5}\}$.

We subtract the integer component that is multiplied to each of the basis element. In other words, we show that $\alpha - 7a - (3+\sqrt{-5})\bar{a}$ can be represented as a $\mathbb{Z}$-combination of the basis.

Consider:

$$\begin{aligned} \alpha - 7a - (3+\sqrt{-5})\bar{a} &= 7b\sqrt{-5} - 5\bar{b} + 3\sqrt{-5}\bar{b} \\ &= 7b(-3) - 5\bar{b} + 3(-3)\bar{b} + 7b(3+\sqrt{-5}) + 3\bar{b}(3+\sqrt{-5}) \\ &= (-3b-2\bar{b})7 + (7b+3\bar{b})(3+\sqrt{-5}) \end{aligned}$$

So indeed α can be expressed as a $\mathbb{Z}$ combination of our basis. Uniqueness follows trivially from comparing the coefficients.

For the ring $\mathbb{Z}[\sqrt{-5}]$, we had shown that the discriminant is 20. Compute the discriminant of I:

$$\Delta[I] = Abs\left(\begin{vmatrix} 7 & 3+\sqrt{-5} \\ 7 & 3-\sqrt{-5} \end{vmatrix}^2\right) = |(14\sqrt{-5})^2| = 980$$

The norm of I is:

$$N(I) = \sqrt{980/20} = 7$$

We search for a element in the ring $\mathbb{Z}[\sqrt{-5}]$ that has a norm of 7. Write:

$$N(\beta) = n^2 + 5m^2 = 7$$

Where $\beta := n + \sqrt{-5}m$ for some integer n, m. Take mod 5. $n^2 \equiv 2(mod\ 5)$ but 2 is not a quadratic residue of 5. Hence, there is no solution for the equation, and no element that has a norm of 7 exists.

Ergo, I is non-principal. □

3. Let I be an ideal of a dedekind domain D. Assume that there exists some $\alpha \in I$ such that $N(I) = |N(\alpha)|$. Prove that $I = \langle\alpha\rangle$.

Proof We know that there exists an ideal I' in D that satisfies:

$$II' = \langle\alpha\rangle$$

for the ideal classes form a group, and $\alpha \in I$. Norms of ideals are multiplicative. Thus:

$$N(I)N(I') = N(\langle\alpha\rangle) = |N(\alpha)|$$

We know that the value of $N(I)$. By cancellation:

$$N(I') = 1$$

Recall the definition of ideal norms. The norm of an ideal is the size of the factor ring created by the entire ring moded out by the ideal. For this case:

$$|D/I'| = 1$$

And thus:

$$I' = D$$

Ergo:

$$II' = ID = I = \langle\alpha\rangle$$

as desired.

□

4. We know that for any prime ideal $\mathfrak{p} \subsetneq \mathcal{O}_K$, it is true that $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$ for some prime number p. We say the ideal $\mathfrak{p}$ lies over p. Moreover, it is possible to write:

$$\mathcal{O}_K\langle p \rangle = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_t^{e_t}$$

The exponents of the ideals, e_i or also denoted as $e(\mathfrak{p}_i|p)$, is called the ramification index of the prime ideal $pideal_i$ over p. Moreover, we observe that $N(\mathfrak{p}_i) = p_k^f i$. f_i is called to be the relative degree of the ideal $\mathfrak{p}_i$ over p. Prove:

$$\sum_{i=1}^{t} e_i f_i = n$$

where $n := [K : \mathbb{Q}]$

Proof

The equation is almost an immediate consequence of applying the norm both sides of the factorization of the ideal $\langle p \rangle$ in the ring $\mathcal{O}_K$. Write:

$$N(\mathcal{O}_K\langle p \rangle) = N(\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_t^{e_t})$$

By the multiplicative property of ideal norms, along with the fact that the norm of a principal ideal equals to the norm of the generator, we deduce:

$$|N(p)| = N(\mathfrak{p}_1^{e_1})N(\mathfrak{p}_2^{e_2})\cdots N(\mathfrak{p}_t^{e_t})$$

And moreover:

$$p^n = N(\mathfrak{p}_1^{e_1})N(\mathfrak{p}_2)^{e_2}\cdots N(\mathfrak{p}_t)^{e_t} = p^{e_1 f_1}p^{e_2 f_2}\cdots p^{e_t f_t}$$

Comparing the powers, we reach the result.

$$n = \sum_{i=1}^{t} e_i f_i$$

□

5. Let p be an odd prime in $\mathbb{Z}$. Let $K = \mathbb{Q}$ be a quadratic field.

i If $p|d$, prove that:

$$\langle p \rangle \mathcal{O}_K = \mathfrak{p}^2$$

for some prime ideal p.

Proof We claim that $\mathfrak{p} := \langle p, \sqrt{d} \rangle$ works. Consider:

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

d is squarefree and $p|d$. We deduce $gcd(p, d/p) = 1$. By Bezout's identity, it is possible to obtain a $\mathbb{Z}$ combination of $p, d/p$ that results in 1. That is, we obtain some $a, b \in \mathbb{Z}$ that satisfies:

$$ap + bd/p = 1$$

Multiplying by p both sides:

$$ap^2 + bd = p$$

This equation shows that

$$p \in \langle p^2, p\sqrt{d}, d \rangle \quad \text{and} \quad \langle p \rangle \subseteq \langle p^2, p\sqrt{d}, d \rangle$$

Also, take any element from $\langle p \rangle$. Write, for arbitrary integer n, m:

$$p(n + m\sqrt{d}) = pn + pm\sqrt{d} = (ap^2 + bd)n + pm\sqrt{d}$$
$$= anp^2 + bnd + mp\sqrt{d} \in \langle p^2, p\sqrt{d}, d \rangle$$

Thus, $\langle p \rangle \subseteq \langle p^2, p\sqrt{d}, d \rangle$ and the two ideals are equivalent.
To show that the chosen candidate is indeed prime, take the norm. Write:

$$N(\langle p, \sqrt{d} \rangle^2) = N(\langle p \rangle) = p^2$$

Thus:

$$N(\langle p, \sqrt{d} \rangle)^2 = p^2$$

It must be:

$$N(\langle p, \sqrt{d} \rangle) = p$$

An ideal with a prime norm must be prime. This concludes the proof. $\square$

ii If $p \nmid d$ and d is square mod p, prove that:

$$\langle p \rangle \mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_2$$

where the two ideals are distinct.

Proof Let $d \equiv r^2 (mod\, p)$ for some integer $0 \leq r < p$. We first conjure two ideals that multiply up to $\langle p \rangle$. Then, we will show that the two ideals are distinct. Consider:

$$\begin{aligned} \langle p, \sqrt{d} - r \rangle \langle p, \sqrt{d} + r \rangle &= \langle p^2, d - r^2, p\sqrt{d} - pr, p\sqrt{d} + pr \rangle \\ &= \langle p^2, 2pr, d - r^2, p\sqrt{d} - pr \rangle \end{aligned}$$

p is an odd prime, and $0 \leq r < p$ so $gcd(p, 2r) = 1$ and by Bezout's identity we obtain two integers a, b that satisfies:

$$ap + 2br = 1 \quad \text{and} \quad ap^2 + 2bpr = p$$

By this equality, we notice that:

$$p \in \langle p^2, 2pr, d - r^2, p\sqrt{d} - pr \rangle \quad \text{and} \quad \langle p \rangle \subseteq \langle p^2, 2pr, d - r^2, p\sqrt{d} - pr \rangle$$

Moreover, take any element from the principal ideal generated by p. Call the element $p\alpha$. Write:

$$p\alpha = a\alpha p^2 + 2b\alpha pr \in \langle p^2, 2pr, d - r^2, p\sqrt{d} - pr \rangle$$

Thus:

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

It remains to show that two ideals are prime and distinct. First, show that the two ideals are distinct. Assume for the sake of contradiction, that two ideals are identical. It follows that

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

and hence:

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

The last equality follows by the Bezout's identity. As a consequence:

$$\langle p \rangle = \langle 1 \rangle \quad \text{and} \quad N(\langle p \rangle) = N(\mathcal{O}_K) \quad \text{and} \quad p^2 = 1$$

Which is a contradiction ϟ

Finally, show that both of the ideals are proper. As a result, we conclude that both of the ideals have a prime norm of p and thus both ideals are prime. Assume for a contradiction that one of the ideal, say $\langle p, \sqrt{d} - r \rangle$ is the entire ring.

It must be:

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

And hence:

$$\sqrt{d} + r \in \langle p \rangle$$

There must be some element α in the ring $\mathcal{O}_K$ that satisfies:

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

and thus, in the field of quotients:

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

and in the field, the multiplicative inverse is unique. Nonetheless, this element is not in the ring itself. We reach a contradiction. The same argument goes for the other ideal.

□

6. Prove that if $p \nmid d$, and d is not a squre mod p, then $\langle p \rangle \mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$

Proposition For any element $\alpha \in \mathcal{O}_K$, assuming the conditions on d, $p|\alpha$ if and only if $p|N(\alpha)$

Proof Start with the foward direction. Write, for some element $\beta \in \mathcal{O}_K$:

$$\alpha = p\beta \quad \text{and} \quad N(\alpha) = p^2 N(\beta)$$

Hence $p|N(\alpha)$.

For the opposite direction, assume $p|N(\alpha)$ but $p \nmid \alpha$ in the ring $\mathcal{O}_K$. Write α in the form of $a + b\sqrt{d}$. Either $p \nmid a$ or $p \nmid b$. Also, from $p|N(\alpha)$, deduce:

$$a^2 - db^2 \equiv 0 (mod\ p) \quad \text{or} \quad a^2 = db^2 (mod\ p)$$

If $p|b$, then $p|a$ and $p|\alpha$ in the ring of integers. Hence assume $p \nmid b$. There must exist a modular inverse of b in mod p. Thus:

$$d = (ab^{-1})^2 (mod\ p)$$

However, the condition of d is that it is not a square mod p. We reach a contradiction, and therefore, $p|\alpha$. □

Solution Assume for a contradiction that $\langle p \rangle \mathcal{O}_K$ is not prime. We obtain some elements $\alpha, \beta, \gamma \in \mathcal{O}_K$ that satisfies:

$$\gamma p = \alpha\beta$$

where $p \nmid \alpha, \beta$ in the ring $\mathcal{O}_K$. Taking the norm both sides:

$$N(\gamma)p^2 = N(\alpha)N(\beta)$$

and thus $p|N(\alpha)$ or $p|N(\beta)$ necessarily. However, by proposition, this implies $p|\alpha$ or $p|\beta$, which is a contradiction. □

Book 5.15 In $\mathbb{Z}[\sqrt{-29}]$:

$$30 = 2 \cdot 3 \cdot 5 = (1 + \sqrt{-29})(1 - \sqrt{-29})$$

i) Show $\langle 30 \rangle \subseteq \langle 2, 1 + \sqrt{-29} \rangle$

Proof Trivially we observe that $1 + \sqrt{-29}$ and $-1 + \sqrt{-29}$ is in the ideal. The negation of the product, 30, must also be in the ideal. Moreover, $\langle 30 \rangle$ must be included in $\langle 2, 1 + \sqrt{-29} \rangle$. □

ii) Verify $\mathfrak{p}_1 := \langle 2, 1 + \sqrt{-29} \rangle$ has a norm of 2 and thus is prime.

Proof We claim that the $\mathbb{Z}$-basis of the ideal $\mathfrak{p}_1$ is $\{2, 1 + \sqrt{-29}\}$. The $\mathbb{Z}$-span of the set must be included in $\mathfrak{p}_1$. Take any element from the ideal and show that it is in the $\mathbb{Z}$-span of the basis.

$$2(a + b\sqrt{-29}) + (1 + \sqrt{-29})(c + d\sqrt{-29})$$

Subtract the $\mathbb{Z}$-multiples, i.e. $2a, (1 + \sqrt{-29})c$. It suffices to show that the following term can be expressed as a $\mathbb{Z}$ combination of the basis:

$$\begin{aligned} 2b\sqrt{-29} - 29d + d\sqrt{-29} &= -29d + (2b + d)\sqrt{-29} \\ &= -30d - 2b + (2b + d)(\sqrt{-29} + 1) \\ &= (-15d - b)2 + (2b + d)(\sqrt{-29} + 1) \end{aligned}$$

And indeed the claimed set spans $\mathfrak{p}_1$. Uniqueness follows from comparing the coeffiecients.

We compute the discriminant of the basis for I and the whole ring:

$$\Delta = Abs(\begin{vmatrix} 1 & \sqrt{-29} \\ 1 & -\sqrt{-29} \end{vmatrix}^2) = |(2\sqrt{-29})^2| = 116$$

$$\Delta[I] = \begin{vmatrix} 2 & 1 + \sqrt{-29} \\ 2 & 1 - \sqrt{-29} \end{vmatrix} = |(4\sqrt{-29})^2| = 4 \cdot 116$$

The norm of I is therefore:

$$N(I) = \sqrt{4 \cdot 116/116} = 2$$

and $\mathfrak{p}_1$ is prime. □

iii) Check $1 - \sqrt{-29} \in \mathfrak{p}_1$ and deduce $\langle 30 \rangle \subseteq p_1^2$

Proof $2 - (1 + \sqrt{-29}) = 1 - \sqrt{-29}$ so it must be in $\mathfrak{p}_1$. Consqeuently, $(1 - \sqrt{-29})(1 + \sqrt{-29}) \in \mathfrak{p}_1^2$ which is equivalent to $30 \in \mathfrak{p}_1^2$. We conlude $\langle 30 \rangle \in \mathfrak{p}_1^2$ □

iv) Factorize the ideal $\langle 30\rangle$ into prime ideals.

Proof First note:

$$\langle 30\rangle = \langle 2\rangle\langle 3\rangle\langle 5\rangle$$

In problem 5-i, we have proved that an ideal $\langle p\rangle$ can be factored as $\langle p, \sqrt{d}\rangle^2$ in a quadratic field $\mathbb{Q}$ where $p \nmid d$ and p is an odd prime, d square mod p. Hence:

$$\langle 3\rangle = \langle 3, \sqrt{-29}+1\rangle\langle 3, \sqrt{-29}-1\rangle \quad \text{and} \quad \langle 5\rangle = \langle 5, \sqrt{-29}+1\rangle\langle 5, \sqrt{-29}-1\rangle$$

Also observe:

$$\langle 2, 1+\sqrt{-29}\rangle\langle 2, 1-\sqrt{-29}\rangle = \langle 4, 30, 2+2\sqrt{-29}, 2-2\sqrt{-29}\rangle$$

$$= \langle 2, 4, 2+2\sqrt{-29}, 2-2\sqrt{-29}\rangle = \langle 2\rangle$$

We have shown previously that $N(\langle 2, 1+\sqrt{-29}\rangle) = 2$ so the norm of the other ideal must also be 2, in order for the two norms to multiply up to $N(\langle 2\rangle) = 4$. In fact, the two ideals are equal to eqch other.

We write the prime factorization of the ideal $\langle 30\rangle$:

$$\langle 30\rangle = \langle 2, 1+\sqrt{-29}\rangle^2\langle 3, \sqrt{-29}+1\rangle\langle 3, \sqrt{-29}-1\rangle\langle 5, \sqrt{-29}+1\rangle\langle 5, \sqrt{-29}-1\rangle$$

The connection between the prime factorization and the 2-3-5 factorization is evident. By some many lines of algebra, it can be deduced that:

$$\langle 1+\sqrt{-29}\rangle = \langle 2, 1+\sqrt{-29}\rangle\langle 3, \sqrt{-29}+1\rangle\langle 5, \sqrt{-5}+1\rangle$$

And also:

$$\langle 1-\sqrt{-29}\rangle = \langle 2, 1+\sqrt{-29}\rangle\langle 3, \sqrt{-29}-1\rangle\langle 5, \sqrt{-5}-1\rangle$$

trust me...

These results relate to the factorization:

$$\langle 30\rangle = \langle 1+\sqrt{-29}\rangle\langle 1-\sqrt{-29}\rangle$$

□