1. Let K be a number field, and let I be an ideal in $\mathcal{O}_k$. If $\alpha \in I$, prove that $N(\alpha) \in I$.

Proof

Recall the definition of $N(\alpha)$.

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

where each $\sigma_i(\alpha)$ are the embedded images of α and n is the degree of the extension. WLOG, we claim that $\sigma_1(\alpha) = \alpha$. If $n = 1$, then the norm of α equals to α and the theorem becomes trivial. Assume $n > 1$.

It suffices to show that the following product is an element of $\mathcal{O}_k$:

$$P := \prod_{i=2}^{n} \sigma_i(\alpha)$$

Notice:

$$N(\alpha) = \alpha \cdot P$$

by strong closure of ideals, $\alpha \in I$ implies the product implies that the Norm is in I. Nonetheless, it must be shown that the product P is in the ring.

Consider the field polynomial of α. It must be a polynomial over $\mathbb{Z}$. Call it $f(t)$. Write:

$$f(t)/(t-\alpha) = \prod_{i=2}^{n} (t - \sigma_i(\alpha))$$

By polynomial long division, we notice that the constant term of the LHS is some constant within $\mathcal{O}_k$. By Viete's relation, that constant term is exactly the desired product P.

$\square$

2. Show in $\mathbb{Z}[\sqrt{-5}]$ that $\sqrt{-5}|(a + b\sqrt{-5})$ iff $5|a$. Deduce that $\sqrt{-5}$ is prime in $\mathbb{Z}[\sqrt{-5}]$. Hence, conclude that the element 5 factors uniquely in this ring, even if the ring is not a UFD.

Proof ($\Leftarrow$) If $5|a$, there exists some element $\xi \in \mathbb{Z}[\sqrt{-5}]$ that satisfies $a = 5\xi$. Thus, $a = -\sqrt{-5} \cdot (\sqrt{-5}\xi)$.

Write:

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

which concludes this side of the proof.

($\Rightarrow$) $\sqrt{-5}|(a + b\sqrt{-5})$ implies $\sqrt{-5}|a$. Again, write a in terms of multiples of ξ.

$$a = \sqrt{-5}\xi$$

Multiply by the algebraic conjugate both side.

$$a^2 = \sqrt{-5} - (\sqrt{-5})(\xi)(\bar{\xi}) = 5N(\xi)$$

Looking at the equation in the ring $\mathbb{Z}$, we conclude that $5|a^2$ and thus $5|a$, for 5 is prime.

Take any two elements α, β in the ring $\mathbb{Z}[\sqrt{-5}]$. Assume that the product is divisible by $\sqrt{-5}$. Write:

$$\alpha := a + b\sqrt{-5}, \beta := c + d\sqrt{-5}$$

$$\alpha\beta = (a + b\sqrt{-5})(c + d\sqrt{-5})$$
$$= ac - 5bd + \sqrt{-5}(ad + bc)$$

The real part of the product must be divisible by 5, by the proposition that we have proven. $5|(ac - 5bd)$ so $5|ac$. WLOG, $5|a$. Again, by the proposition, $\sqrt{-5}|\alpha$ as desired.

Move on to factorize 5. $5 = -(\sqrt{-5})^2$. Any irreducible factorization of 5 must include two associates of $\sqrt{-5}$. Assume we have another factorization that has more irreducibles other than these two associates. After cancellation, we are left with a set of irreducibles that multiply up to a unit, which is impossible for all irreducibles are nonunits. We conclude that the factorization is unique up to associates.

3. Show that $Q(\sqrt{-d})$ is not a UFD where $d = 2, 3(mod 4)$ and $d = 0(mod 5)$, d squarefree.

Solution

For utility, we will show that $\sqrt{-5n}|(a + b\sqrt{-5n})$ iff $5n|a$.

Start with the forward direction. Write $d = -5n$. Since d is squarefree, n is also a squarefree integer. $\sqrt{-5n}|(a + b\sqrt{-5n})$ implies $\sqrt{-5n}|a$. Again, write a in terms of multiples of ξ.

$$a = \sqrt{-5n}\xi$$

Multiply by the algebraic conjugate both side.

$$a^2 = \sqrt{-5n} - (\sqrt{-5n})(\xi)(\bar{\xi}) = 5nN(\xi)$$

Looking at the equation in the ring $\mathbb{Z}$, we conclude that $5n|a^2$ and thus $5n|a$, for $5n$ is squarefree.

Move on to the backwards

4. Consider the ring $\mathrm{R} = \mathbb{Z}[\sqrt{-3}]$. Let $I :=< 2, 1 + \sqrt{-3} >$ be an ideal in R.

(i) Prove that $I \neq< 2 >$ in R

<u>Proof</u> The element $1 + \sqrt{-3}$ is in the ideal I, but it is not in $< 2 >$. Assume for a contradiction, $1 + \sqrt{-3} \in< 2 >$. For some element $\xi \in R$:

$$1 + \sqrt{-3} = 2\xi$$

Write $\xi = a + b\sqrt{-3}$ where a, b are integers.

$$1 + \sqrt{-3} = 2a + 2b\sqrt{-3}$$

The coefficients must match, so $2a = 1$ for some integer a. There is no integer solution, and we conclude that $1 + \sqrt{-3}$ is not in $< 2 >$

(2) Prove that $I^2 =< 2 > I$

<u>Proof</u> Recall the identity:

$$< a, b >^2 =< a^2, ab, b^2 >$$

Rewrite the LHS:

$$I^2 =< 2, 1+\sqrt{-3} >^2 =< 4, 2+2\sqrt{-3}, 1-3+2\sqrt{-3} > =< 4, 2+2\sqrt{-3}, 2-2\sqrt{-3} >$$

Notice:

$$4 - (2 + 2\sqrt{-3}) = 2 - 2\sqrt{-3}$$

We write:

$$I^2 =< 4, 2 + 2\sqrt{3} >$$

Moving on the the RHS:

$$< 2 > I =< 2 >< 2, 1 + \sqrt{-3} > =< 4, 2 + 2\sqrt{-3} >$$

We conclude:

$$I^2 =< 2 > I$$

(iii) Is R a dedekind domain?

<u>Claim</u> No R is not a dedekind domain.

<u>Proof</u> First establish two propositions. First of all, 2 is irreducible in the ring R. Assume for a contradiction that 2 is reducible. Write:

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = 2$$

where $a, b, c, d \in \mathbb{Z}$

Multiplying both sides by the algebraic conjugate, we get:

$$(a^2 + 3b^2)(c^2 + 3d^2) = 2 \cdot \bar{2} = 4$$

If either one of the two terms equal 1, then $(a, b) = (\pm 1, 0)$ or $(c, d) = (\pm 1, 0)$ which in case shows that 2 is irreducible. Thus, we consider $(a^2 + 3b^2) = 2$. However, this equation has no integer solution, since $|b| < 1$ but then $a^2 = 0$ which has no solution.

The second proposition is that I is a proper ideal. It suffices to show that $1 \notin I$. Assume $1 \in I$ for a contradiction. Write:

$$2(a + b\sqrt{-3}) + (1 + \sqrt{-3})(c + d\sqrt{-3}) = 1$$

Where $a, b, c, d \in \mathbb{Z}$ Comparing coefficients, we deduce:

$$2a + c + 3d = 1$$

$$2b - c + d = 0$$

Adding up, we get:

$$2a + 4d = 1$$

But the LHS is even while the RHS is odd. We have reached a contradiction and indeed I is proper.

I is not a dedekind domain. The ideal $< 2 >$ is a prime ideal, for 2 is irreducible. Clearly, $< 2 > \subsetneq < 2, 1 + \sqrt{-3} > = I$. On part(1), we showed that the two ideals are distinct. By the proposition established, I is a proper Ideal. Thus $< 2 >$ is a prime ideal that is not maximal. R is not a dedekind domain. $\square$

5. In domain D, a principal ideal $< p >$ is prime iff p is zero or prime.

Proof $(\Leftarrow)$ If $p = 0$, then the ideal $< p > = 0$. The zero ideal must be prime, for integral domians don't have zero divisor. Suppose p is prime, but $< p >$ is not a prime ideal. It is possible to obtain two elements $a, b \in D$ such that $a, b \notin < p >$ but $ab \in p$. This means $p|ab$. Since p is prime, $p|a$ WLOG. This implies $a \in < p >$ which is a contradiction.

$(\Rightarrow)$ Assume that $< p >$ is a prime ideal, but p is nonzero and nonprime. For p is nonprime, write:

$$pq = ab$$

for $a, b \in D$ which are nonzero and nonunits, and some $q \in D$. Recall that in a domain, an ideal is prime iff the domain mod ideal is also a domain. Since $< p >$ is domain by assumption, the fractional domain $D / < p >$ must have no zero divisors.

We claim that $a+ < p >$ and $b+ < p >$ are zero divisors. Clearly, both of them are nonzero by assumption. Write:

$$(a+ < p >)(b+ < p >) = ab+ < p >$$

and notice that $ab \in < p >$ so indeed the coset is the zero coset. $\square$