MAT415 Assignment 1 Solutions

September 29, 2020

Problem 1 (Exercise 1.13 Pg. 11)**.** *Let d be a squarefree integer. Then the ring of integers $\mathcal{O}_K$ in $K = \mathbb{Q}(\sqrt{d})$ is:*

$$\mathbb{Z}[\sqrt{d}] \textit{ if } d \equiv 2, 3 \pmod 4$$

$$\mathbb{Z}[\tfrac{1+\sqrt{d}}{2}] \textit{ if } d \equiv 1 \pmod 4$$

Solution. Let $\alpha = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ for $r, s \in \mathbb{Q}$. The minimal polynomial of α is:

$$(X - r - s\sqrt{d})(X - r + s\sqrt{d}) = X^2 - 2rX + (r^2 - ds^2).$$

Now, $\alpha \in \mathcal{O}_K$ if and only if its minimal polynomial has integer coefficients if and only if $2r \in \mathbb{Z}$ and $r^2 - ds^2 \in \mathbb{Z}$. We note that $2r$ and $2s$ are both integers (since $2r$ is an integer, $2s\sqrt{d} = 2\alpha - 2r$ belongs to $\mathcal{O}_K$, which means that $d(2s)^2$ is an integer, but since d is square-free, $2s$ must already be an integer). So $r = \frac{a}{2}$ and $s = \frac{b}{2}$ with a and b integers. So $\alpha \in \mathcal{O}_K$ is equivalent to our equation is equivalent to

$$a^2 - db^2 \in 4\mathbb{Z}.$$

Looking at this equation modulo 4, this is equivalent to $a^2 = db^2 \pmod 4$. Now, the quadratic residues modulo 4 are $\{0, 1\}$.

If $d \equiv 2, 3 \pmod 4$, this is equivalent to $a^2 \equiv b^2 \equiv 0 \pmod 4$ which is equivalent to asking for a, b to be even, which is same as asking for r, s to be integers. This means that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \pmod 4$.

If $d \equiv 1 \pmod 4$, this is equivalent to asking for $a^2 \equiv b^2 \pmod 4$ which is equivalent to asking that $a \equiv b \pmod 2$. This means that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \pmod 4$. $\square$

Problem 2 (Exercise 1.29 on Pg. 16)**.** *Prove that $\mathbb{Z}[\sqrt{-3}]$ is not a Dedekind domain, and does not admit unique factorization of ideals.*

Solution. Note that $\mathbb{Z}[\sqrt{-3}]$ is a Noetherian integral domain with Krull dimension 1. This is because it is the quotient of the dimension 2 Noetherian ring $\mathbb{Z}[x]$ by the prime ideal $(x^2 + 3)$. So the only thing that could go wrong is being integrally closed. Looking at Problem 1, we see that $\frac{1+\sqrt{-3}}{2}$ is integral and lies in the fraction field of $\mathbb{Z}[\sqrt{-3}]$ but not in $\mathbb{Z}[\sqrt{-3}]$.

The fact that unique factorization of ideals fails in $\mathbb{Z}[\sqrt{-3}]$ will be done in Problem 6. $\square$

Problem 3 (Exercise 1.37 on Pg. 20)**.** *A Dedekind ring is a UFD if and only if it is a PID.*

Solution. The direction [$\Leftarrow$] is easy since any PID is a UFD.

The direction [$\Rightarrow$] needs more work since UFDs don't need to be PIDs. For example, $\mathbb{Z}[x]$ is a UFD but not a PID (why?).

Suppose that R is a Dedekind ring which is a UFD. We want to show that R is a PID. First, we claim that it suffices to show that every prime ideal is principal. Indeed, if every prime ideal is principal and I is an ideal of R, then since R is a Dedekind ring, we can write $I = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ for some unique prime ideals $\mathfrak{p}_i$. But products of principal ideals are principal and so I is principal.

We now show that every prime ideal of R is principal. The (0) ideal is prime and principal. Consider a prime ideal $(0) \neq \mathfrak{p}$. Let $0 \neq x \in \mathfrak{p}$ be an element and write $x = p_1 \cdots p_l$ for irreducible elements p_i by using the UFD property. Then since $\mathfrak{p}$ is prime, at least one of the p_i must belong to $\mathfrak{p}$, say p_{i_0}. But then the ideal (p_{i_0}) is prime (since irreducible elements are prime in a UFD) and fits in the chain $(0) \subsetneq (p_{i_0}) \subseteq \mathfrak{p}$. Since Dedekind domains have Krull dimension 1, the containment $(p_{i_0}) \subset \mathfrak{p}$ must be an equality. Therefore, $\mathfrak{p}$ is principal. $\square$

Problem 4 (Exercise (1) on Pg. 30)**.** *Prove that the following rings are not UFDs by explicitly finding two distinct factorizations of the same element.*

a) $\mathbb{Z}[\sqrt{-13}]$

b) $\mathbb{Z}[\sqrt{10}]$

Solution. a) We have $14 = 2 \cdot 7 = (1 + \sqrt{-13})(1 - \sqrt{-13})$. We now check that $2, 7, 1 \pm \sqrt{-13}$ are irreducible. The norm equation is $N(a + b\sqrt{-13}) = a^2 + 13b^2$. We can check by inspection that there are no elements of norm 2 or 7. We now check that this implies that 2 is irreducible. If 2 were reducible we could write it as $2 = \alpha\beta$ for some elements α and β which are not units. But then $4 = N(2) = N(\alpha)N(\beta)$. Since α and β are not units, neither can have norm ± 1 and thus both have norm 2. But this is a contradiction since we have shown that there are no elements of norm 2. Similarly, one can show that 7 and $1 \pm \sqrt{-13}$ are irreducible.

b) We have $6 = 2 \cdot 3 = (2 + \sqrt{10})(-2 + \sqrt{10})$. The norm equation is $N(a + b\sqrt{10}) = a^2 - 10b^2$. Taking the equation modulo 10, we see that we get a quadratic residue modulo 10. The quadratic residues modulo 10 are $\{1, 4, 5, 6, 9\}$. Therefore, there are no elements of norm 2 or 3 and thus $2, 3, \pm 2 + \sqrt{10}$ are all irreducible.

$\square$

Problem 5 (Exercise (5) on Pg. 30)**.** *This problem has two parts.*

a) Determine the ring of integers in $\mathbb{Q}(\sqrt{d})$ *for all square-free integers* d*.*

b) Determine the unit group of the ring of integers in $\mathbb{Q}(\sqrt{d})$ *for all square-free integers* $d < 0$*.*

Solution. a) In Problem 1, we found that the ring of integers $\mathcal{O}_K$ in $K = \mathbb{Q}(\sqrt{d})$ is:

$$\mathbb{Z}[\sqrt{d}] \text{ if } d \equiv 2, 3 \pmod 4$$

$$\mathbb{Z}[\tfrac{1+\sqrt{d}}{2}] \text{ if } d \equiv 1 \pmod 4.$$

b) To find the units of $\mathbb{Q}(\sqrt{d})$ for all square-free integers $d < 0$, we solve the norm equation $N(u) = 1$ in $\mathcal{O}_K$.

If $d \equiv 2, 3 \pmod 4$, we need to find all $a, b \in \mathbb{Z}$ such that

$$N(a + b\sqrt{d}) = a^2 - db^2 = 1.$$

This equation has only the trivial solutions $(a, b) = (\pm 1, 0)$, except when $d = -1$, where the solutions are $(a, b) = (\pm 1, 0)$ and $(a, b) = (0, \pm 1)$.

If $d \equiv 1 \pmod 4$, we need to find all $a, b \in \mathbb{Z}$ with $a \equiv b \pmod 2$ such that

$$N(\tfrac{a+b\sqrt{d}}{2}) = \frac{a^2 - db^2}{4} = 1.$$

This is equivalent to finding all $a, b \in \mathbb{Z}$ with $a \equiv b \pmod 2$ such that

$$a^2 - db^2 = 4.$$

This equation has only the trivial solutions $(a, b) = (\pm 2, 0)$, except when $d = -3$, where the solutions are $(a, b) = (\pm 2, 0)$ and $(a, b) = (\pm 1, \pm 1)$.

Recall that any finite subgroup of the unit group of a field is cyclic. Therefore, our calculations tell us that the unit group of $\mathbb{Q}(\sqrt{d})$ for square-free integers $d < 0$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, with the exception of $\mathbb{Q}(i)$ where it is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and of $\mathbb{Q}(\sqrt{-3})$ where it is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

As you will see, imaginary quadratic fields are the only number fields whose unit group is finite.

□

Problem 6 (Exercise (7) on Pg. 31). *Let $R = \mathbb{Z}[\sqrt{-3}]$, and let I be the ideal of R generated by 2 and $1 + \sqrt{-3}$.*

a) Show that $I^2 = (2)I$ but $I \neq (2)$. Conclude that proper ideals in R do not factor uniquely into products of prime ideals.

b) Show that I is the unique prime ideal of R containing (2). Conclude that the ideal (2) cannot be written as a product of prime ideals of R.

c) Why do parts (a) and (b) above not contradict the theorem which says that every Dedekind domain admits unique factorization of proper ideals into products of prime ideals?

Solution. a) We have $I = (2, 1 + \sqrt{-3})$. We find

$$I^2 = (4, 2 + 2\sqrt{-3}, -2 + 2\sqrt{-3}) = (4, 2 + 2\sqrt{-3}) = (2)I.$$

To see that $I \neq (2)$, note that $1 + \sqrt{-3} \in I$ and any $a + b\sqrt{-3} \in (2)$ must have a, b even.

Note that I is prime since $R/I \cong \mathbb{Z}/2\mathbb{Z}$ is a field.

If R had unique factorization into prime ideals, we could write $(2) = \mathfrak{p}_1 \cdots \mathfrak{p}_m$ for some prime ideals $\mathfrak{p}_j$ with more than one equal I or at least one of them different from I. Then, we would have $I^2 = I\mathfrak{p}_1 \cdots \mathfrak{p}_l$. This is a contradiction to uniqueness of factorisation into prime ideals since either the power of I would not match on both sides or a prime ideal factor would appear on the right side but not on the left side.

b) The prime ideals of R containing (2) are in bijection with the prime ideals of $R/(2) \cong (\mathbb{Z}/2\mathbb{Z})[\sqrt{-3}]$. But $(\mathbb{Z}/2\mathbb{Z})[\sqrt{-3}]$ has 4 elements, namely $0, 1, \sqrt{-3}, 1 + \sqrt{-3}$. Furthermore, you can check that 1 and $\sqrt{-3}$ are the only units of $(\mathbb{Z}/2\mathbb{Z})[\sqrt{-3}]$. Thus $(\mathbb{Z}/2\mathbb{Z})[\sqrt{-3}]$ has a unique prime ideal $(1 + \sqrt{-3})$. This means that I is the unique prime ideal of R containing (2).

If you could write (2) as a product of primes, then the only prime that would show up would be I since it is the only prime ideal which contains (2). But then, $(2) = I^k$ for some exponent $k > 1$. But then from part (a), we would find $(2) = I^k = (2^{k-1})I$. This is a contradiction since $(2^{k-1})I = (2^k, 2^{k-1} + 2^{k-1}\sqrt{-3})$ does not contain 2 for $k > 1$.

c) As shown in Problem 2, $\mathbb{Z}[\sqrt{-3}]$ is not a Dedekind domain because it is not integrally closed.

□