Question: 11

Let $\mathbb{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

a. Prove that $\mathbb{Z}[\sqrt{2}\,]$ is an integral domain.

b. Find all the units of $\mathbb{Z}[\sqrt{2}\,]$.

c. Determine the field of fractions of $\mathbb{Z}[\sqrt{2}\,]$.

d. Prove that $\mathbb{Z}[\sqrt{2}i\,]$ is a Euclidean domain under the Euclidean valuation $\nu(a + b\sqrt{2}\,i) = a^2 + 2b^2$.

Solution:

a. Consider $(a+b\sqrt{2})(c+d\sqrt{2}) = 0$. This means that $(a+b\sqrt{2})(a-b\sqrt{2})(c+d\sqrt{2})(c-d\sqrt{2}) = (a^2-2b^2)(c^2-2d^2) = 0$. The irrationality of $\sqrt{2}$ and that fact that a, b, c, d are all integers tells us that either $a = b = 0$ or $c = d = 0$. 😄

b. If u is a unit, then so are $-u, 1/u$, and $-1/u$. At least one of these has to be greater than 1 if $u \neq 0$. As such, it is enough to show that if $u < 1$, then u is a power of $1+\sqrt{2}$. So, we can write that $(1+\sqrt{2})^k < u < (1+\sqrt{2})^{k+1}$. Dividing by $(1+\sqrt{2})^k$ gives us $1 < u(1+\sqrt{2})^{-k} < 1+\sqrt{2}$. Since $1+\sqrt{2}$ is the smallest unit not equal to $0, u(1+\sqrt{2})^{-k} = 1 \Rightarrow u = (1+\sqrt{2})^k$. Since norm is multiplicative, we have that all powers of $1+\sqrt{2}$ are units.

c.
$$Q = \left\{\frac{a + b\sqrt{2}}{c + d\sqrt{2}} : a, b, c, d \in \mathbb{Z}, c + d\sqrt{2} \neq 0\right\}$$

d. We first need to show that $\nu(xy) = \nu(x)\nu(y)$ for $x, y \in \mathbb{Z}[\sqrt{2i}]$.

$$\begin{aligned}
\nu((a + b\sqrt{2i})(c + d\sqrt{2i})) &= \nu((ac - 2bd) + (ad + bc)\sqrt{2i}) \\
&= (ac - 2bd)^2 + 2(ad + bc)^2 \\
&= a^2c^2 + 2a^2d^2 + 2b^2c^2 + 4b^2d^2 \\
\nu(a + b\sqrt{2i})\nu(c + d\sqrt{2i}) &= (a^2 + 2b^2)(c^2 + 2d^2) \\
&= a^2c^2 + 2a^2d^2 + 2b^2c^2 + 4b^2d^2
\end{aligned}$$

For nonzero values, we have that $\nu(x) \geqslant 1$ and it follows that $\nu(x) \leqslant \nu(xy)$.

Next, let $a + b\sqrt{2i}, c + d\sqrt{2i} \in \mathbb{Z}[\sqrt{2i}]$ with nonzero $c + d\sqrt{2i}$. Now define q_1 to be the closest integer to $\frac{ac}{c^2}$ and q_2 as the closest integer to $\frac{bc}{c^2}$. Define s_1, s_2, r_1, r_2 as follows:

$$s_1 + s_2\sqrt{2i} = \left(\frac{ac + 2bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + 2d^2}\sqrt{2i}\right) - (q_1 + q_2\sqrt{2i})$$

$$r_1 + r_2\sqrt{2i} = (a + b\sqrt{2i}) - \left(q_1 + q_2\sqrt{2i}\right)(c + d\sqrt{2i})$$

From this, we need to show that $r_1^2 + 2r_2^2 < c^2 + 2d^2$. Start by noting that $|s_1|, |s_2| \leqslant \frac{1}{2}$ by definition of q_1 and q_2. So,

$$(s_1 + s_2\sqrt{2i})(c + d\sqrt{2i}) = (a + b\sqrt{2i}) - (q_1 + q_2\sqrt{2i})(c + d\sqrt{2i}) = r_1 + r_2\sqrt{2i}$$

Thus,

$$\nu(r_1 + r_2\sqrt{2i}) = \nu(s_1 + s_2\sqrt{2i})\nu(c + d\sqrt{2i}) \leqslant \left(\frac{1}{4} + 2 \cdot \frac{1}{4}\right)\nu(c + d\sqrt{2i}) < \nu(c + d\sqrt{2i})$$

Therefore, the original statement was proved and also we proved that $\mathbb{Z}[\sqrt{2i}]$ is a Euclidean domain. 😄

Question: 17

Prove or disprove: Every subdomain of a UFD is also a UFD.

Solution: $\mathbb{Z}[3i] \subseteq \mathbb{C}$ is a subdomain of a UFD, but is not a UFD. 😊

Question: 18

An ideal of a commutative ring R is said to be ***finitely generated*** if there exist elements $a_1, \ldots, a_n$ in R such that every element r in the ideal can be written as $a_1 r_1 + \cdots + a_n r_n$ for some $r_1, \ldots, r_n$ in R. Prove that R satisfies the ascending chain condition if and only if every ideal of R is finitely generated.

Solution: We start by proving that if R satisifes ACC, then its ideals are finitely generated. Let I be a nonzero ideal and a_1 a nonzero value of I. If $I = \langle a_1 \rangle$, then I is finitely generated. If not, then $I_1 = \langle a_1 \rangle$ is a subset of I. Now consider $a_2 \in I \backslash I_1$. Let, $I_2 = \langle a_1, a_2 \rangle$. If $I = I_2$, we are done. If not, we have an $a_3 \in I \backslash I_2$ and we continue the process to have that $I_1 \subseteq I_2 \subseteq I_3 \cdots$. By ACC, there exists an N such that $I_n = I_N$ for all $n \geqslant N$. But if $I_{N+1} = I_N$, then there are no elements in I that aren't in I_N. Therefore, $I = \langle a_1, \ldots, a_N \rangle$ and I is finitely generated.

For the converse, we supposed the ideals of R are finitely generated. We have that $I = \bigcup_{n=1}^{\infty} I_n$ is an ideal. But since every ideal is finitely generated, we have that $I = \langle a_1, \ldots, a_k \rangle$ for some k. But then for $n = 1, 2, 3, \cdots k$, $a_i \in I_{b_i}$ for some integer b_i. Let $N = \max(b_1, \ldots, b_k)$. Then $a_i \in I_{b_i} \subseteq I_N$. Therefore, $I \subseteq I_N$. So, $I_n = I_N$ for all $n \geqslant N$ and R satisfies ACC. 😊

Question: 19

Let D be an integral domain with a descending chain of ideals $I_1 \supset I_2 \supset I_3 \supset \cdots$. Suppose that there exists N such that $I_k = I_N$ for all $k \geqslant N$. A ring satisfying this condition is said to satisfy the ***descending chain condition***, or DCC. Rings satisfying the DCC are called ***Artinian rings***, after Emil Artin. Show that if D satisfies the descending chain condition, it must satisfy the ascending chain condition.

Solution: Consider $I_i = \langle a^k \rangle$ for some $a \in D$. Since $a^{n+1}d = a^n(ad)$, we have that $a^{n+1} \subseteq a^n D$. So, we have a descending chain of ideals as follows:

$$aD \supseteq a^2 D \supseteq \ldots \supseteq a^n D \supseteq a^{n+1} D \supseteq \ldots$$

which stabilizes since D is Artinian. So, we can say that

$$a^{m+1} D = a^m D$$

for some positive integer m. Since $a^m = a^m 1_D \in D$, there exists b such that $a^{m+1} = a^m b$, or that $a^m(1_D - ab) = 0$. This yields that $ab = 1_D$ as $a, a^m \neq 0$ since D is an integral domain. We have shown that $a \neq 0 \in D$ has an inverse and as such, D is a field which satisifies the ascending chain condition. 😊