ALGEBRAIC STRUCTURES TUTORIAL WEEK 22

Question. Prove that $\mathbb{Z}[\sqrt{-5}]$ is a subring of $\mathbb{C}$. Is it a subfield of $\mathbb{C}$?

Background material.

Definition 0.1. A *ring* is a set R together with two operations on R, usually written as *addition* $a+b$ and *multiplication* $a \cdot b$, such that
(i) R with addition is an abelian group;
(ii) R is closed with respect to multiplication;
(iii) multiplication is associative, i.e. $a(bc) = (ab)c$ for every $a, b, c \in R$;
(iiv) multiplication is distributive over addition, i.e.

$$a(b+c) = ab + ac \quad \text{and} \quad (a+b)c = ac + bc$$

for all $a, b, c \in R$. The above are called that *distributive laws.*

Theorem 0.2. *A subset S of a ring R is a subring of R if and only if*
(a) S is non-empty;
(b) S is closed under both the addition and the multiplication of R; and
(c) S contains the negative of each of its elements.

Example 0.3. Let $F = M(\mathbb{R})$ denote the ring of all functions $f : \mathbb{R} \to \mathbb{R}$. Let S denote the set of all $f \in F$ such that $f(1) = 0$. We shall use Theorem 0.2 to prove that S is a subring of F.

Now we have $0_F \in S$ where $0_F(x) = 0$ for all $x \in \mathbb{R}$ because $0_F(1) = 0$. Therefore S is non-empty.

For $f, g \in S$, we have

$$(f+g)(1) = f(1) + g(1) = 0 + 0 = 0$$

and

$$(fg)(1) = f(1)g(1) = 0 \cdot 0 = 0,$$

therefore $f+g$ and fg are in S. Hence we have closure for both operations.

Lastly for $f \in S$, we have $f(1) = 0$, and so $(-f)(1) = -f(1) = -0 = 0$. Therefore $-f \in S$. Hence the negative of each element in S is again in S.

Definition 0.4. A commutative ring in which the set of non-zero elements form a group with respect to multiplication is called a *field.*

Definition 0.5. A subset K of a field F is a *subfield* of F if K is itself a field with respect to the operations on F.

Theorem 0.6. *A subset K of a field F is a subfield of F if and only if*
(a) K contains the zero and unity of F;
(b) if $a, b \in K$, then $a + b \in K$ and $ab \in K$;
(c) if $a \in K$, then $-a \in K$; and
(d) if $a \in K$ and $a \neq 0$, then $a^{-1} \in K$.

Example 0.7. $\mathbb{Q}$ is a subfield of $\mathbb{R}$. Both $\mathbb{Q}$ and $\mathbb{R}$ are subfields of $\mathbb{C}$. The ring $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$. The ring $\mathbb{Z}[\sqrt{2}]$ is an integral domain but not a field: for example, $-2+\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, but $(-2+\sqrt{2})^{-1} = -1 - \frac{1}{2}\sqrt{2} \notin \mathbb{Z}[\sqrt{2}]$.