§1 11-06

Definition 1.1. A subring of a ring is a subset $S \subseteq R$ such that $(S, +, \cdot)$ is itself a ring (some operations are restricted).

Example 1.2

$5\mathbb{Z} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Proposition 1.3

A subset $S \subseteq R$ is a ring if and only if:

1. $S \neq \varnothing$
2. Let $x, y \in S$, then $x - y \in S$. (If this is true, then the set contains the identity element, whenever an element is inside its inverse is inside, whenever two elements are in S its product is in S. This is just a faster way of showing these).
3. Let $x, y \in S$, then $x \cdot y \in S$.

What about associativity and distributive, etc? Those properties are inherited from the ring.

Example 1.4

$$2\mathbb{Z}_{10} \subseteq \mathbb{Z}_{10}$$

$$\{0, 2, 4, 6, 8\} \subset \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Yes, this is a subring but it does not have unity because it does not include "1".

$$S \neq \varnothing, \qquad x - y \in S, \qquad x \cdot y \in S$$

Example 1.5

$$\mathbb{Z}[x^2] \subseteq \mathbb{Z}[x]$$

$$\mathbb{Z}[x^2] = \{a_{2n}x^{2n} + a_{2(n-1)}x^{2(n-1)} + \cdots + a_0x^0\}$$

i.e. $\mathbb{Z}[x^2]$ represents polynomials where the odd polynomial coefficients are 0.

Yes, this is a subring and it has unity because it contains "1", the identity element.

$$S \neq \varnothing, \qquad x - y \in S, \qquad x \cdot y \in S$$

Example 1.6

$$T_{n\times n}(\mathbb{R}) \subset M_{n\times n}(\mathbb{R})$$

$T_{n\times n}(\mathbb{R})$ which represents upper triangular matrices. i.e. zeros bellow diagonal.

$$\begin{bmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{bmatrix}$$

Yes a subring.

§1.1 Integral domains and fields

Definition 1.7. The subring $\mathbb{Z}[i] \subset \mathbb{C}$ consisting of $\{m + ni : m, n \in \mathbb{Z}\}$ is the Gaussian Integers.

Remark 1.8. Not every Gaussian Integer is a unit in the Gaussian Integers. Indeed, ± 1 and $\pm i$ are the only units. Proof:

Suppose $\alpha, \beta \in \mathbb{Z}[i]$, and $\alpha\beta = 1$ where $\alpha = a_1 + a_2 i$ and $\beta = b_1 + b_2 i$. Remember that for $z_1 = a_1 + b_1 i$ and $z_2 = a_2 + b_2 i$:

$$\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$$

Then if follows that

$$1 = 1 \cdot 1 = (\alpha\beta)(\overline{\alpha\beta}) = (\alpha\beta)(\overline{\alpha}\,\overline{\beta}) = (\alpha\overline{\alpha})(\beta\overline{\beta}) = (a_1^2 + a_2^2)(b_1^2 + b_2^2)$$

Hence $(a_1^2 + a_2^2) = \pm 1$ and $(b_1^2 + b_2^2) = \pm 1$.

$\mathbb{Z}[i]$ is an integral domain since it is the subring of a field with unity which implies that the subring is an integral domain.

$$xy = 0 \Rightarrow x = 0 \vee y = 0$$

because $x^{-1}xy = x^{-1}0 \Rightarrow y = 0$.

Example 1.9

$\mathbb{Z}_p$ is a field with p elements.

Theorem 1.10

There exista a field with p^n elements for each $n \geq 1$ when p is prime.

Example 1.11

$$M_{2\times 2}(\mathbb{Z}_2) \supset \mathbb{F}_4 = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\}$$

is a field with 2^2 elements.

Proposition 1.12

Let D be a commutative ring with "1" i.e. unity.

Then D is an integral domain if and only if for all non zero $a \in D$, $(ab = ac) \Rightarrow (b = c)$

Proof.

$(\Rightarrow)$

$$ab = ac \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$$

$(\Leftarrow)$

$$ab = 0 \Rightarrow ab = a0 \Rightarrow b = 0$$

because $a \neq 0$

□