Lecture 02: Subring criterion

Monday, April 2, 2018 1:08 PM

At the end of the previous lecture we mentioned a subring criterion:

. Suppose $(A,+,\cdot)$ is a ring. Then $B \subseteq A$ is a subring if and only if (1) $(B,+)$ is a subgroup, (2) B is closed under multiplication. As we combine this with a subgroup criterion we get the following:

Proposition (Subring criterion) Suppose $(A,+,\cdot)$ is a ring, and $B \subseteq A$. Then B is a subring if and only if $\forall\, b_1, b_2 \in B$ (1) $b_1 - b_2 \in B$ and (2) $b_1 \cdot b_2 \in B$.

Ex. $n\mathbb{Z}$ is a subring of $\mathbb{Z}$ which is not unital if $n>1$.

Ex. $M_n(\mathbb{Q}) :=$ the set of $n \times n$ rational matrices with the usual addition and multiplication of matrices.

In fact for any ring R, $M_n(R)$ is a ring (Check why.)

Ex./Def. Suppose $R_1, \ldots, R_n$ are rings. Then the direct product $R_1 \times \cdots \times R_n$ is a ring with componentwise operations; that means

$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$ and

Lecture 02: Examples and zero divisors

Wednesday, April 4, 2018 1:23 PM

$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n)$.

Notice if 1_{R_i} is the unity of R_i for $1 \le i \le n$, then $(1_{R_1}, \dots, 1_{R_n})$ is the unity of $R_1 \times \cdots \times R_n$.

__Ex.__ Compute $(1,0) \cdot (1,\sqrt{2})$ in $\mathbb{Z} \times \mathbb{R}$;

$$(1,0) \cdot (1,\sqrt{2}) = (1,0).$$

__Ex.__ Compute $(1,0) + (1,\sqrt{2})$ in $\mathbb{Z} \times \mathbb{R}$;

$$(1,0) + (1,\sqrt{2}) = (2,\sqrt{2}).$$

__Ex.__ Compute $\begin{bmatrix} (1,0) & (1,\sqrt{2}) \\ (0,1) & (1,1) \end{bmatrix}^2$ in $M_2(\mathbb{Z} \times \mathbb{R})$.

$$\begin{bmatrix} (1,0) & (1,\sqrt{2}) \\ (0,1) & (1,1) \end{bmatrix} \begin{bmatrix} (1,0) & (1,\sqrt{2}) \\ (0,1) & (1,1) \end{bmatrix} =$$

$$\begin{bmatrix} (1,0)(1,0)+(1,\sqrt{2})(0,1) & (1,0)(1,\sqrt{2})+(1,\sqrt{2})(1,1) \\ (0,1)(1,0)+(1,1)(0,1) & (0,1)(1,\sqrt{2})+(1,1)(1,1) \end{bmatrix} =$$

$$= \begin{bmatrix} (1,0)+(0,\sqrt{2}) & (1,0)+(1,\sqrt{2}) \\ (0,0)+(0,1) & (0,\sqrt{2})+(1,1) \end{bmatrix} = \begin{bmatrix} (1,\sqrt{2}) & (2,\sqrt{2}) \\ (0,1) & (1,1+\sqrt{2}) \end{bmatrix}$$

Lecture 02: zero-divisors; ring of integers mod n

Wednesday, April 4, 2018 2:29 PM

Remark. $(0,1)\cdot(1,0)=(0,0)$; so sometimes product of two non-zero elements is zero. Such elements are called zero-divisors.

Def: Suppose A is a commutative ring. $a\in A\setminus\{0\}$ is called a zero-divisor if $\exists\, b\in A\setminus\{0\}$ s.t. $ab=0$.

Ex. $(1,0)$ is a zero-divisor in $\mathbb{Z}\times\mathbb{R}$.

Pf. $(1,0)(0,1)=(0,0)$.

Ex. The ring $\mathbb{Z}_n$ of integers modulo n. I am going to follow your book and use a bit non-standard way of defining $\mathbb{Z}_n$.

$\mathbb{Z}_n=\{0,1,\dots,n-1\}$ as set.

Division algorithm $m\in\mathbb{Z}$, $n\in\mathbb{Z}^+$, $\exists!\,(q,r)\in\mathbb{Z}\times\mathbb{Z}$, (a) $m=nq+r$ (b) $0\le r<n$.

(q is called the quotient of m divided by n and r is called the remainder.)

For $a,b\in\mathbb{Z}_n$, $a\oplus b:=$ the remainder of $a+b$ divided by n.

Lecture 02: Congruence arithmetic

Wednesday, April 4, 2018 8:20 AM

and $a \odot b :=$ the remainder of $a \cdot b$ divided by n.

To see why $\mathbb{Z}_n$ is a ring, let us recall basic properties of congruence arithmetic from your previous courses:

<u>Def.</u> • For $a, b \in \mathbb{Z}$, we say $a \mid b$ if $b = ak$ for some $k \in \mathbb{Z}$

• For $n \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, we say $a \equiv b \pmod{n}$ if $n \mid a-b$. (We say a is congruent to b modulo n)

<u>Basic Properties of Congruence arithmetics</u>

(1) $a \equiv a \pmod{n}$; $\left.\begin{array}{l} a_1 \equiv a_2 \pmod{n} \\ a_2 \equiv a_3 \pmod{n} \end{array}\right\} \Rightarrow a_1 \equiv a_3 \pmod{n}$.

(2) $\left.\begin{array}{l} a_1 \equiv a_2 \pmod{n} \\ b_1 \equiv b_2 \pmod{n} \end{array}\right\} \Rightarrow a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$

(3) $\left.\begin{array}{l} a_1 \equiv a_2 \pmod{n} \\ b_1 \equiv b_2 \pmod{n} \end{array}\right\} \Rightarrow a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}$

(4) r is the remainder of a divided by if and only if $a \equiv r \pmod{n}$ and $r \in \{0, 1, \ldots, n-1\}$.

Lecture 02: Basic properties of congruence arithmetic

Monday, April 2, 2018 11:06 AM

Pf. (1) $\left.\begin{array}{l} n \mid 0 \\ a-a=0 \end{array}\right\} \Rightarrow n \mid a-a$; and so $a \equiv a \pmod{n}$.

$$\left.\begin{array}{l} a_1 \equiv a_2 \pmod{n} \Rightarrow n \mid a_1-a_2 \Rightarrow a_1-a_2 = nk \text{ for some } k \in \mathbb{Z} \\ a_2 \equiv a_3 \pmod{n} \Rightarrow n \mid a_2-a_3 \Rightarrow a_2-a_3 = n\ell \text{ for some } \ell \in \mathbb{Z} \end{array}\right\}$$

$$\Rightarrow (a_1-a_2)+(a_2-a_3) = nk+n\ell = n(\underbrace{k+\ell}_{\text{in } \mathbb{Z}})$$

$$\Rightarrow n \mid a_1-a_3 \Rightarrow a_1 \equiv a_3 \pmod{n}.$$

(2) $a_1 \equiv a_2 \pmod{n} \Rightarrow n \mid a_1-a_2 \Rightarrow a_1-a_2 = nk$ for some $k \in \mathbb{Z}$.

$b_1 \equiv b_2 \pmod{n} \Rightarrow n \mid b_1-b_2 \Rightarrow b_1-b_2 = n\ell$ for some $\ell \in \mathbb{Z}$.

$$\Rightarrow \left.\underbrace{(a_1-a_2)+(b_1-b_2)}_{(a_1+b_1)-(a_2+b_2)} = n(k+\ell)\right\} \Rightarrow a_1+b_1 \equiv a_2+b_2 \pmod{n}.$$

(3) As in part (2), $a_1-a_2 = nk$ and $b_1-b_2 = n\ell$ for some k,ℓ in $\mathbb{Z}$. Then

$$a_1b_1 - a_2b_2 = a_1b_1 - a_2b_1 + a_2b_1 - a_2b_2$$

$$= (a_1-a_2)b_1 + a_2(b_1-b_2)$$

We will continue next time.