추상대수학 1 20181288 [illegible].

Sec 3.1

32. We need to check four conditions of $Z(R)$ to be substring of R.

Let $a, b \in Z(R)$ and $r \in Z(R)$

(i) $(a+b)r = ar + br = ra + rb = r(a+b)$.

This means $(a+b) \in Z(R)$.

(ii) $(ab) \cdot r = a \cdot (br) = a \cdot (rb) = (ar) \cdot b$

$= (ra) \cdot b = r(ab)$.

This means $(ab) \in Z(R)$

cancellation law.

(iii) $0 \cdot r = (0+0) \cdot r = 0 \cdot r + 0 \cdot r \rightarrow 0 \cdot r = 0$.

$r \cdot 0 = r(0+0) = r \cdot 0 + r \cdot 0 \rightarrow r \cdot 0 = 0$

This means $0 \in Z(R)$.

(iv) We first need to prove $(-a)\cdot b = -(ab) = a\cdot(-b)$.

Consider $(-a)\cdot b + a\cdot b = ((-a)+a)\cdot b$

$$= 0\cdot b = 0.$$

By above, ab's additive inverse is $(-a)\cdot b$, which means $(-a)\cdot b = -(ab)$

We could also get $a\cdot(-b) = -(ab)$ by the way above.

Let's use this result.

$(-a)\cdot r = -(ar) = -(ra) = r(-a)$.

This means $-a \in Z(R)$.

By (i), (ii), (iii) and (iv), $Z(R)$ is a subring of R $\blacksquare$

38. Let $r_1, r_2 \in A_R$ and $a \in R$.

(i) $a \cdot (r_1 + r_2) = ar_1 + ar_2 = 0_R + 0_R = 0_R$

$\therefore (r_1 + r_2) \in A_R$

(ii) $a \cdot (r_1 r_2) = (ar_1) \cdot r_2 = 0_R \cdot r_2 = 0_R$

$\therefore r_1 r_2 \in A_R$

(iii) $0_R \cdot a = 0_R \quad \therefore 0_R \in A_R$

(iv) $a(-r_1) = -(ar_1) = -0_R = 0_R$

$\therefore$ if $r_1 \in A_R$, then $-r_1 \in A_R$

By (i), (ii), (iii), and (iv) A_R is a subring of R. ∎

42. (a) Since R is a division ring, $b \in R$ has a multiplicative inverse b^{-1}. Thus, $bb^{-1} = b^{-1}b = 1_R$.

$$1_R = bb^{-1} = bbb^{-1} = b \cdot (bb^{-1}) = b\,1_R = b.$$

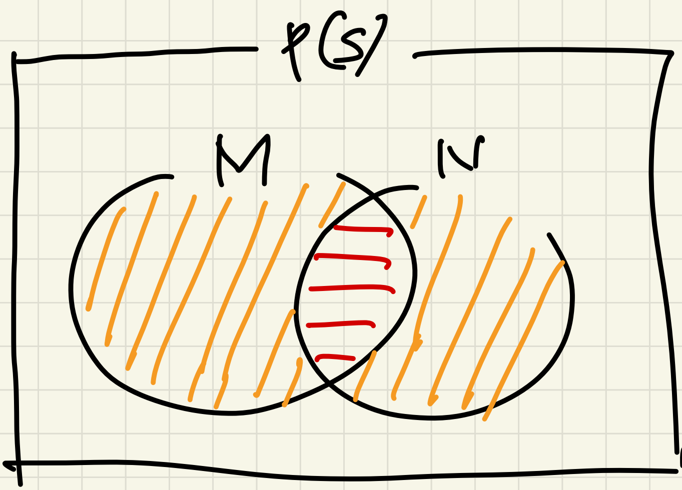
$\therefore b = 1_R$ ∎

(b) $ua \cdot ua = u \cdot (au) \cdot a = u 1_R \cdot a$

$= ua$

By (a), $ua = 1_R$ ∎

44.



$M + N \subset P(S)$

$MN \subset P(S)$

→ closure under addition and multiplication.

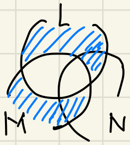
$M+N = (M-N) \cup (N-M) = (N-M) \cup (M-N)$

$= N+M$ → commutative under addition.

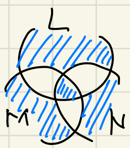
$MN = M \cap N = N \cap M = NM$

→ commutative under multiplication

Let $L, M, N \in P(S)$

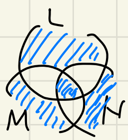


$L+M$



$(L+M)+N$

$M+N$



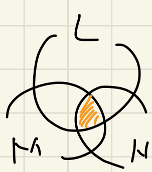
$L+(M+N)$

→ associative under addition.

LM

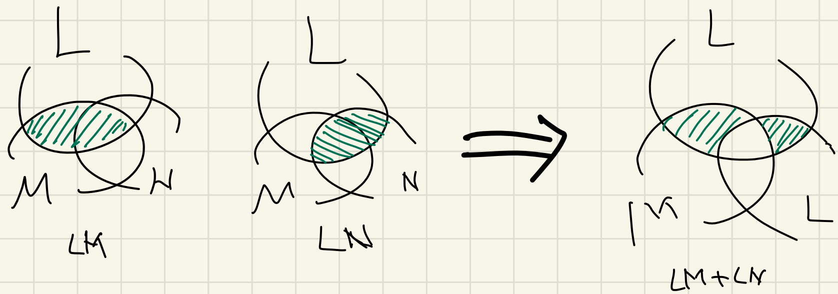
$(LM)N$

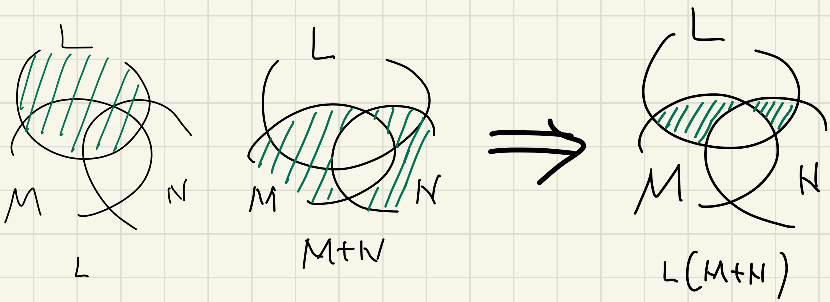
MN



$L(MN)$

→ associative under multiplication





Thus, $LM+LN = L(M+N)$ and

$ML+NL = LM+LN = L(M+N) = (M+N)L$.

→ distributive law holds

$M+\phi = (M-\phi) \cup (\phi-M) = M \cup \phi = M$

→ ϕ is the additive identity.

$M+M = (M-M) \cup (M-M) = \phi \cup \phi = \phi$.

→ M is the additive inverse of $M \in P(S)$.

$MS = M \cap S = M$

$\rightarrow$ S is the multiplicative identity of $P(S)$.

(b) $x^2 = x \cap x = x$

$x + x = (x - x) \cup (x - x) = \phi \cup \phi = \phi = 0_{P(S)}$

Sec 3.2

34. (a) (i) If A is invertible, $ad - bc \neq 0_F$

$\Leftrightarrow$ If $ad - bc = 0_F$, then A is not invertible

Consider $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

The above means that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a zero divisor, not a unit.

Thus A is not invertible ∎

(ii) If $ad-bc \neq 0_F$, then A is invertible.

Consider $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Then, there exists a multiplicative inverse of A when $ad-bc \neq 0$,

and multiplicative inverse is always unique, $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ is the only multiplicative inverse of A.

Thus, the statement is true

By (i),(ii), A is invertible iff

$ad-bc \neq 0$ ∎

(b) If A is a zero divisor, $ad-bc=0$.

By (a), if A is not invertible, $ad-bc=0$

we could say that

if A is a zero divisor, $ad-bc=0$.

If $ad-bc=0$, A is a zero divisor.

Consider $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$

if $ad-bc=0$, the result would be $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

which means, A is a zero divisor. ∎

40. ($\Rightarrow$) Let's think of contrapositive.

If 0_R is not a unique solution for the equation, then we can think of $a \neq 0_R$ s.t $a^2 = 0_R$. This means a is a nonzero nilpotent element $\boxed{R}$

($\Leftarrow$) Suppose $a \neq 0_R$, $n > 1$ s.t

$a^n = 0_R$, always set minimal n.

if $n=2$, $a^2 = 0_R$ so the equation holds.

if $n \geq 3$, $a^n = 0_R$, then $a^{n-1} \neq 0_R$.

$$(a^{n-1})^2 = a^{2n-2} = a^n \cdot a^{n-2} = 0 \cdot a^{n-2} = 0$$

which is a contradiction that 0_R is the only solution.

44. (a) Let $a^m = 0$, $b^n = 0$ for $m, n \in \mathbb{N}$.

$(a+b)^k = {}_kC_0 \cdot a^k \cdot b^0 + {}_kC_1 a^{k-1} b^1 + \cdots + {}_kC_k \cdot a^0 b^k$

get an arbitrary term and that would be ${}_kC_r \cdot a^{k-r} b^r$.

If we set $k = m+n-1$, $k-r \geq m$ and $r \geq n$.

This means $a^{k-r} = 0$ or $b^r = 0$.

Thus $(a+b)^k = 0_R + 0_R + \cdots + 0_R = 0_R$.

$(ab)^{mn} = a^{mn} \cdot b^{mn} = (a^m)^n \cdot (b^n)^m$

$= (0_R)^n \cdot (0_R)^m = 0_R \cdot 0_R$

$= 0_R$ ▫

(b) Let $a, b \in N$ then by (a),

(i) $a+b \in N$, (ii) $ab \in N$.

(iii) 0_R is obviously a nilpotent element

(iv) if $a \in N$, then $-a \in N$

because $a^m = 0$ then $-a^m = 0$.

$$(-a)^m = \begin{cases} a^m & (m: \text{even}) \\ -a^m & (m: \text{odd}) \end{cases}$$

$$= 0.$$

By (i), (ii), (iii), and (iv), N is a subring of R ■