08.04.2024 ①
Algebra Lect 9/6
A.Ram

$\sup(E)$ and $\inf(E)$

Let S be a set.

A relation on S is a subset L of $S\times S$

If $x,y\in S$ and $(x,y)\in L$ then write $x\le y$

A poset, or partially ordered set, is a set S with a relation $\le$ such that

(a) if $x,y\in S$ and $x\le y$ and $y\le z$ then $x\le z$

(b) if $x,y\in S$ and $x\le y$ and $y\le x$ then $x=y$.

Let $(S,\le)$ be a poset. Let $E\subseteq S$.

The supremum of E is $\sup(E)$ such that

(a) $\sup(E)\in S$ and $\sup(E)$ satisfies
  if $x\in E$ then $x\le \sup(E)$

(b) If $b\in S$ and b satisfies
  if $x\in E$ then $x\le b$
 then $\sup(E)\le b$.

The infimum of E is $\inf(E)$ such that

(a) $\inf(E)\in S$ and $\inf(E)$ satisfies
  if $x\in E$ then $x\ge \inf(E)$

(b) If $b\in S$ and b satisfies
  if $x\in E$ and $x\ge b$
 then $\inf(E)\ge b$.

$P+Q$ and $P\cap Q$

Let R be a ring. Let M be an R-module. Let N be an R-submodule of M. Define

$$\mathcal{S}_{[N,M]} = \left\{ \begin{matrix} R\text{-modules } P \text{ with} \\ N \subseteq P \subseteq M \end{matrix} \right\}$$

partially ordered by inclusion.

Let $P, Q \in \mathcal{S}_{[N,M]}$. Define

$$P+Q = \{p+q \mid p\in P \text{ and } q \in Q\} \quad \text{and}$$

$$P\cap Q = \{m \in M \mid m\in P \text{ and } m \in Q\}.$$

Proposition

$$P+Q = \sup(P,Q) \quad \text{and} \quad P\cap Q = \inf(P,Q)$$

Proof sketch: To show:

(a) $P \subseteq P+Q$ and $Q \subseteq P+Q$

(b) If $L \in \mathcal{S}_{[N,M]}$ and $P \subseteq L$ and $Q \subseteq L$ then $P+Q \subseteq L$

(c) $P\cap Q \subseteq P$ and $P \cap Q \subseteq Q$

(d) If $K \in \mathcal{S}_{[N,M]}$ and $K \subseteq P$ and $K \subseteq Q$ then $K \subseteq P\cap Q$.

gcd and lcm

Let R be a UFD and let $x, y \in R$.

The greatest common divisor of x and y is $\gcd(x,y)$ such that

(a) $\gcd(x,y) \in R$ and $\gcd(x,y)$ divides x and $\gcd(x,y)$ divides y.

(b) If $d \in R$ and d divides x and d divides y then d divides $\gcd(x,y)$.

The least common multiple of x and y is $\mathrm{lcm}(x,y)$ such that

(a) $\mathrm{lcm}(x,y) \in R$ and $\mathrm{lcm}(x,y)$ is a multiple of x and $\mathrm{lcm}(x,y)$ is a multiple of y.

(b) If $m \in R$ and m is a multiple of x and m is a multiple of y then m is a multiple of $\mathrm{lcm}(x,y)$.

Rewrite the definition of $\gcd(x,y)$ in terms of principal ideals.

(a) $\gcd(x,y) \in R$ and $\gcd(x,y)R \supseteq xR$ and $\gcd(x,y)R \supseteq yR$

(b) If $d \in R$ and $dR \supseteq xR$ and $dR \supseteq yR$ then $dR \supseteq \gcd(x,y)R$.

If R is a PID then

$$\gcd(x,y)R = xR + yR = \sup(xR, yR)$$

$$\mathrm{lcm}(x,y)R = xR \cap yR = \inf(xR, yR)$$

in $\mathcal{S}_{[0,R]}$.

If R is a UFD and $p_1, \ldots, p_\ell \in R$ are irreducible and $a_1, \ldots, a_\ell, b_1, \ldots, b_\ell \in \mathbb{Z}_{\geq 0}$ and

$$x = p_1^{a_1} \cdots p_\ell^{a_\ell} \quad \text{and} \quad y = p_1^{b_1} \cdots p_\ell^{b_\ell}$$

then

$$\gcd(x,y) = p_1^{\min(a_1,b_1)} \cdots p_\ell^{\min(a_\ell,b_\ell)} \quad \text{and}$$

$$\mathrm{lcm}(x,y) = p_1^{\max(a_1,b_1)} \cdots p_\ell^{\max(a_\ell,b_\ell)}$$

Note that $\gcd(x,y)$ and $\mathrm{lcm}(x,y)$ are determined only up to mutiplication by units.

<u>Proposition</u> (modular law) Let R be a ring and M an R-module and N a submodule of M. Let $\mathcal{S}_{[N,M]} = \left\{ \begin{matrix} R\text{-modules } P \text{ with} \\ N \subseteq P \subseteq M \end{matrix} \right\}$ partially ordered by inclusion.

Let $P, Q, L \in \mathcal{S}_{[N,M]}$.

If $P \subseteq Q$ then $Q \cap (P+L) = P + (Q \cap L)$.

The modular law

Let R be a ring and let M be an R-module. Let N be an R-submodule of M. Let

$$\mathcal{S}_{[N,M]} = \left\{ \begin{array}{c} R\text{-modules } P \text{ with} \\ N \subseteq P \subseteq M \end{array} \right\}$$

partially ordered by inclusion.

Let $P, Q \in \mathcal{S}_{[N,M]}$. Then

$$\sup(P,Q) = P+Q \quad \text{and} \quad \inf(P,Q) = P \cap Q.$$

Proposition (modular law). Let $P, Q, L \in \mathcal{S}_N^M$.

If $P \subseteq Q$ then $Q \cap (P+L) = P + (Q \cap L)$

(Think: $\mathrm{lcm}(q, \gcd(p,\ell)) = \gcd(p, \mathrm{lcm}(q,\ell))$)

Proof: Assume $P \subseteq Q$.

To show: (a) $Q \cap (P+L) \subseteq P + (Q \cap L)$.

(b) $P + (Q \cap L) \subseteq Q \cap (P+L)$

(a) Assume $a \in Q \cap (P+L)$.

Then $a \in Q$ and there exist $p \in P$ and $\ell \in L$ such that $a = p + \ell$.

To show: $a \in P + (Q \cap L)$.

Since $p \in P \subseteq Q$ and $a \in Q$

then $\ell = a - p \in Q$.

So $l \in Q \cap L$ and $a = p + l \in P + (Q \cap L)$.

So $Q \cap (P+L) \subseteq P + (Q \cap L)$.

Algebra
Lect 18
A. Ram

(b) To show: $P + (Q \cap L) \subseteq Q \cap (P+L)$.

Assume $b \in P + (Q \cap L)$.

To show: $b \in Q \cap (P+L)$.

Since $b \in P + (Q \cap L)$ then there exist $p \in P$ and $l \in Q \cap L$ such that
$$b = p + l.$$

Since $p \in P \subseteq Q$ and $l \in Q$ then
$$b = p + l \in Q.$$

So $b \in Q \cap (P+L)$.

So $P + (Q \cap L) \subseteq Q \cap (P+L)$.

So if $P \subseteq Q$ then $P + (Q \cap L) \subseteq Q \cap (P+L)$. //