3.12 Lecture 16: gcd, lcm, sup, inf, $P+Q$, $P\cap Q$

3.12.1 sup and inf

Let S be a set.

- A **relation** on S is a subset $\angle$ of $S\times S$. If $x,y\in S$ and $(x,y)\in\angle$ write $x\angle y$.

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

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

A **totally ordered set** is a poset such that if $x,y\in S$ then $x\le y$ or $y\le x$.

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

- A **supremum of** E, or **least upper bound of** E, is $\sup(E)$ such that
  (a) $\sup(E)\in S$ and $\sup(E)$ satisfies the condition: if $x\in E$ then $x\le\sup(E)$, and
  (b) If $b\in S$ satisfiles the condition: if $x\in E$ then $x\le b$, then $\sup(S)\le b$.
- A **infimum of** E, or **greatest lower bound of** E, is $\inf(E)$ such that
  (a) $\inf(E)\in S$ and $\inf(E)$ satisfies the condition: if $x\in E$ then $\inf(E)\le x$, and
  (b) If $b\in S$ satisfles the condition: if $x\in E$ then $x\le b$, then $b\le\inf(S)$.

HW: Give an example of a subset of $\mathbb{Q}$ such that $\sup(E)$ does not exist.

3.12.2 $P+Q$ and $P\cap Q$

Proposition 3.61. *Let R be a ring and let M be an R-module. Let N be an R-submodule of M. Define*

$$\mathcal{S}_N^M=\{P\mid N\subseteq P\subseteq M \text{ are } R\text{-module inclusions}\}\qquad \text{partially ordered by inclusion.}$$

For $P,Q\in\mathcal{S}_N^M$, define

$$P+Q=\{p+q\mid p\in P \text{ and } q\in Q\}\qquad\text{and}\qquad P\cap Q=\{m\in M\mid m\in P\text{ and } m\in Q\}$$

(a) Let $P,Q\in\mathcal{S}_N^M$. Then

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

(b) (modular law) If $L,P,Q\in\mathcal{S}_N^M$ and $P\subseteq Q$ then $Q+(L\cap P)=(Q+L)\cap P$.

3.12.3 gcd and lcm

A **unique factorization domain** (or **UFD**) is an integral domain R such that

(a) If $x\in R$ then there exist irreducible $p_1,\ldots,p_n\in R$ such that $x=p_1\cdots p_n$.

(b) If $x\in R$ and $x=p_1\cdots p_n=uq_1\cdots q_m$ where $u\in R$ is a unit and $p_1,\ldots,p_n,\ \ q_1,\ldots,q_m\in R$ are irreducible then $m=n$ and there exists a permutation $\sigma\colon\{1,2,\ldots,n\}\to\{1,2,\ldots,n\}$ and units $u_1,\ldots,u_n\in R$ such that

$$\text{if } i\in\{1,\ldots,n\}\text{ then } q_i=u_ip_{\sigma(i)}.$$

Let R be a unique factorization domain and let $x, y \in R$.

- A **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 $d \in R$ satisfies and d divides x and d divides y then d divides $\gcd(x, y)$.
- A **least common multiple of** x **and** y is $\mathrm{lcm}(x, y)$ such that
  (a) $\mathrm{lcm}(x, y)$ 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 then m is a multiple of $\mathrm{lcm}(x, y)$.

The following proposition says that if R is a UFD then sups and infs exist in the poset

$$\mathcal{P}_0^R = \{\text{principal ideals of } R\} \qquad \text{partially ordered by inclusion.}$$

Proposition 3.62. *Let R be a unique factorization domain and let $x, y \in R$. Then*

(a) $\gcd(x, y)$ *exists and* $\mathrm{lcm}(x, y)$ *exists.*

(b) $\gcd(x, y)$ *and* $\mathrm{lcm}(x, y)$ *are unique up to multiplication by a unit.*

HW:. Let $\mathbb{A}$ be a PID and let $x, y \in \mathbb{A}$. Show that

$$\gcd(x, y)\mathbb{A} = x\mathbb{A} + y\mathbb{A} \qquad \text{and} \qquad \mathrm{lcm}(x, y)\mathbb{A} = x\mathbb{A} \cap y\mathbb{A}.$$

HW:. Let R be a UFD and let $x, y \in R$. Show that if $x, y \in R$ 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

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

then

$$\gcd(x, y) = p_1^{\min(a_1, b_1)} \cdots p_\ell^{\min(a_\ell, b_\ell)} \qquad \text{and} \qquad \mathrm{lcm}(x, y) = p_1^{\max(a_1, b_1)} \cdots p_\ell^{\max(a_\ell, b_\ell)}.$$

HW: Let R be a UFD and let $n \in \mathbb{Z}_{>0}$ and $a_0, \ldots, a_n \in R$. Define $\gcd(a_0, \ldots, a_n)$ and $\mathrm{lcm}(a_0, \ldots, a_n)$ and show that they exist and are unique up to multiplication by units.

3.12.4 Some proofs

Proposition 3.63. *Let R be a ring and let M be an R-module. Let N be an R-submodule of M. Define*

$$\mathcal{S}_N^M = \{P \mid N \subseteq P \subseteq M \text{ are } R\text{-module inclusions}\} \qquad \text{partially ordered by inclusion.}$$

For $P, Q \in \mathcal{S}_N^M$, define

$$P + Q = \{p + q \mid p \in P \text{ and } q \in Q\} \qquad \text{and} \qquad P \cap Q = \{m \in M \mid m \in P \text{ and } m \in Q\}$$

(a) Let $P, Q \in \mathcal{S}_N^M$. Then

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

(b) (modular law) If $L, P, Q \in \mathcal{S}_N^M$ and $P \subseteq Q$ then $Q + (L \cap P) = (Q + L) \cap P$.

Proof.
(a) To show: (aa) $P \subseteq P + Q$ and $Q \subseteq P + Q$.
(ab) If $L \in \mathcal{S}_N^M$ and $P \subseteq L$ and $Q \subseteq L$ then $P + Q \subseteq L$.
(ac) $P \cap Q \subseteq P$ and $P \cap Q \subseteq Q$.
(ad) If $K \in \mathcal{S}_N^M$ and $K \subseteq P$ and $K \subseteq Q$ then $K \subseteq P \cap Q$.
(b) To show: If $P \subseteq Q$ then $Q \cap (P + L) = P + (Q \cap L)$. Assume $P \subseteq Q$.
To show: $Q \cap (P + L) = P + (Q \cap L)$.
To show: (ba) $Q \cap (P + L) \subseteq P + (Q \cap L)$.
To show: (bb) $P + (Q \cap L) \subseteq Q \cap (P + L)$.

(ba) Assume $a \in Q \cap (P + L)$.
To show: $a \in P + (Q \cap L)$.
So there exist $p \in P$ and $\ell \in L$ such that $a = p + \ell$.
Since $a \in Q$ and $p \in Q$ then $\ell = a - p \in Q$.
So $\ell \in Q \cap L$.
So $a = p + \ell \in P + (Q \cap L)$.
So $Q \cap (P + L) \subseteq P + (Q \cap L)$.

(bb) 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 $\ell \in Q \cap L$ such that $b = p + \ell$.
Since $P \subseteq Q$ then $p \in Q$.
So $b = p + \ell \in Q \cap (P + L)$.
So $P + (Q \cap L) \subseteq Q \cap (P + L)$.

$P + (Q \cap L) = Q \cap (P + L)$. □