Operations on Ideals

An ideal is a special subset of a ring. The concepts of ideals was first proposed by Richard Dedekind in 1876. A generalization of the concept of ideal numbers was developed by Ernst Kummer, Later the concept was expanded by David Hilbert and especially Emmy Noether.

Product of an ideal with a set:
Let J be an ideal of a ring R and X be any subset of R. So, the product is defined by,

$$JX = \left\{ \sum_{i=1}^{n} a_i x_i \mid n \geq 1 \; and \; a_i \in J, x_i \in X \; \forall \; i \right\}.$$

Similarly we can define the product of an ideal with finite family of sets.

Theorem:
Let J be an ideal of R and X be any subset of R. Then JX is an ideal of R.

Proof:
We have $JX = \{\sum_{i=1}^{n} a_i x_i \mid n \geq 1 \; and \; a_i \in J, x_i \in X \; \forall \; i\}$. Let, $\sum_{i=1}^{n} a_i x_i, \quad \sum_{i=1}^{n} b_i x_i \in JX$. Since J is an ideal, $-b_i \in J$. That is $\sum_{i=1}^{n} a_i x_i - \sum_{i=1}^{n} b_i x_i = \sum_{i=1}^{n} a_i x_i + \sum_{i=1}^{n} (-b_i) x_i \in JX$. Also $r \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} (r a_i) x_i \in JX$. Hence JX is an ideal.

Note:
The intersection of two ideals of J and K is same as set theoretic intersection of J and K.

Theorem:
The intersection of any family $(J_i)_{i \in I}$ of ideals of a ring R is an ideal.

Proof:
Let $J = \bigcap_{i \in I} J_i$ be an intersection of any family $(J_i)_{i \in I}$ of ideals (where I is an indexing set, finite or otherwise). Let $x, y \in J$, we have to prove $x - y \in J$ and $rx \in J$ for any $x, y \in J$ and $r \in R$. Since $x, y \in J_i$ for each $i \in I$. Since each J_i is an ideal, $x - y \in J_i$ and $rx \in J_i$. That implies $x - y \in J$ and $rx \in J$. That is J is an ideal.

Definition of Ideal generated by a set:
Let R be a ring, and consider $X \subseteq R$. Then ideal generated by X denoted by $\langle X \rangle = \bigcap \{J | X \subseteq J, J \text{ is an ideal of } R\}$.

Example:
Consider the ring of integers $\mathbb{Z}$ with usual addition and multiplication. Then Let $X = \{2\}$. Then $\langle 2 \rangle = 2\mathbb{Z}$. Since we have the ideals of $\mathbb{Z}$ are $n\mathbb{Z}$ and the smallest ideal containing 2 is $2\mathbb{Z}$.

The notion of ideals generated by subsets of a ring is analogous to that of sub groups generated by subsets of a group. Since the intersection of any non empty collection of

ideals of R is also an ideal and X is always contained in at least one ideal (namely R) we have

$$\langle X\rangle = \bigcap_{\substack{I \text{ an ideal} \\ X\subseteq I}} I$$

Definition of Left Ideal Generated by a Set:
The left ideal generated by a set X is the intersection of all left ideals of R that contains X.

Result:
Let X be a subset of a ring R. Then XR is the right ideal generated by X.

Proof:
It is immediate from the definition that RX is closed under addition and under left multiplication by any ring element. Since R has an identity, RX contains X. Thus RX is a left ideal of R which contains X. Conversely, any left ideal which contains X must contain all finite sums of elements of the form $ra, r \in R$ and a $a \in X$ A and so must contain RX. Thus RX is precisely the left ideal generated by X.

We can also define right ideal generated by X. Similarly we can proveXR is the right ideal generated by X and RXR is the (two-sided) ideal generated by A. In particular, if R is commutative then $RX = XR = RXR = \langle X\rangle$.

Note: When R is a commutative ring and $x \in R$, the principal ideal $\langle x\rangle$ generated by x is just the set of all R-multiples of x. If R is not commutative, however, the set $\{axb|a, b \in R\}$ is not necessarily the two-sided ideal generated by a since it need not be closed under addition in this case the ideal generated by x is the ideal RxR, which consists of all finite sums of elements of the form $\{axb|a, b \in R\}$.

The formation of principal ideals in a commutative ring is a particularly simple way of creating ideals, similar to generating cyclic subgroups of a group. Notice that the element $b \in R$ belongs to the ideal $\langle x\rangle$ if and only if $b = rx$ for some $r \in R$, i.e. if and only if b is a multiple of x or, put another way, x divides b in R. Also, $b \in \langle x\rangle$ if and only if $\langle b\rangle \subseteq \langle x\rangle$. Thus, containment relations between ideals, in particular between principal ideals, are seen to capture some of the arithmetic of general commutative rings.

Examples:

- The trivial ideal $\langle 0\rangle$ and the ideal R are both principal Since $0 = \langle 0\rangle$ and $R = \langle 1\rangle$.
- In $\mathbb{Z}$, we have $n\mathbb{Z} = \mathbb{Z}n = \langle n\rangle = \langle -n\rangle$ for all integers n. Thus our notation for R is consistent with the definition of $n\mathbb{Z}$ we have been using. These are all the ideals of $\mathbb{Z}$ so every ideal of $\mathbb{Z}$ is principal. For positive integers n and m, $n\mathbb{Z} \subset m\mathbb{Z}$ if and only if m divides n in $\mathbb{Z}$, so the lattice of ideals containing $n\mathbb{Z}$ is the same as the lattice of divisors of n. Furthermore the ideal generated by two nonzero integers n and m is the principal ideal generated by their greatest common divisor, that is $\langle\{m, n\}\rangle = \langle g.c.d(\{m, n\})\rangle$. The notation for $\langle n, m\rangle$ as the greatest common

divisor of n and m is thus consistent with the same notation for the ideal generated by n and m. In particular, n and m are relatively prime if and only if $\langle n, m\rangle = \langle 1\rangle$.

Remark:
The principle ideal generated by x in a ring R is the product of R and $\{x\}$.

Justification:
We have the principle ideal generated by x, $Rx = \{ax | a \in R\}$. That is $Rx = R\{x\}$.

Example:
We show that the ideal $\langle 2, x\rangle$ generated by 2 and x in $\mathbb{Z}[x]$ is not a principal ideal. Observe that $\langle 2, x\rangle = \{2p(x) + xq(x) | p(x), q(x) \in \mathbb{Z}[x]\}$ and so this ideal consists precisely of the polynomials with integer coefficients whose constant term is even, in particular, this is a proper ideal. Assume by way of contradiction that $\langle 2, x\rangle = \langle p(x)\rangle$ for some $p(x) \in \mathbb{Z}[x]$. Since $2 \in \langle p(x)\rangle$there must be some $q(x)$ such that $2 = q(x)p(x)$. The degree of $q(x)p(x)$ equals degree $q(x)$ + degree $p(x)$, hence both $q(x)$ and $p(x)$ must be constant polynomials, i.e. integers. Since 2 is a prime number, $q(x), p(x) \in \{\pm 1, \pm 2\}$. If $p(x)$ were ± 1 then every polynomial would be a multiple of $p(x)$, contrary to $\langle p(x)\rangle$ being a proper ideal. The only possibility is $p(x) = \pm 2$. But now $x \in \langle p(x)\rangle = \langle 2\rangle = \langle -2\rangle$ and so $x = 2a(x)$ for some polynomial $a(x)$ with integer coefficients, clearly impossible. This contradiction proves that $\langle 2, x\rangle$ is not principal.

Note:
The symbol $\langle X\rangle$ is ambiguous if the ring is not specified. The ideal generated by 2 in $\mathbb{Q}[x]$ is the entire ring $\langle 1\rangle$ since it contains the element $\frac{1}{2} \cdot 2 = 1$.

Definition of Product of ideals:
Let $J_1, \dots, J_k$ be ideals of R. Then $J_1 \cdot J_2 \cdots J_k = \langle x_1, \dots, x_k \, | x_j \in J_j \; forall \; i, j\rangle = \left\{\sum_{i=1}^{n} x_{i1}, \dots, x_{ik} \middle| n \geq 1, x_{ij} \in J_j \forall i, j\right\}$.

Definition of Powers of ideals:
It is a particular case of product of ideals, is defined as,
$J^0 = R$
$J^1 = J$
$J^k = J \cdot J \cdots J \; (k \; times) = \langle x_1 \dots x_k | x_1, \dots, x_k \in J\rangle$.

Definition of Sum of Ideals:
Let I and J be any ideals of R. Then the sum of ideals I and J, $I + J = \{x + y | x \in I, y \in J\}$. It is the smallest ideal containing I and J. More genarally, we may define the sum $\sum_{i \in I} J_i$ of any family of ideals J_i of A; its elements are all sums $\sum x_i$, where $x_i \in J_i$ for all $i \in I$. It is the smallest ideal of R which contains all the ideals J_i.

Note that $J + y$ is the coset of J containing y and $J + y = J + \{y\}$.

Definition of Union of ideals:
Union of ideals is same as union of sets.
Note: The union of two ideals need not be an ideal.

Example:
Consider the ring of integers $\mathbb{Z}$ and $J = \langle 2 \rangle$ and $K = \langle 3 \rangle$. Then $J \cup K \subseteq Z$ is not an ideal, as it is already not a subgroup of the additive group of R, as can be seen by taking $-2 \in J$ and $3 \in K$, and computing $-2 + 3 = 1 \notin J \cup K$.

Result:
Let J and K be two ideals of a ring R. Then $J + K = \langle J \cup K \rangle$
Proof:
Since $J + K \supseteq J \cup K$ and $J + K$ is the smallest ideal containing J and K, we have $J + K = \langle J \cup K \rangle$.

Theorem:
The union of two ideals is an ideal only if one of the ideals is contained within the other.

Proof:
Let the ideal J and K be two ideals. Then $J \cup K$ is an ideal only if for all $x \in J$ and $y \in K, x + y \in J \cup K$. If $J \not\subset K$ and $K \not\subset J$, then there is some $x \in J$ and $x \notin K$ and $y \in K$ and $y \notin J$. That is $x + y \in J$ or $x + y \in K$. If $x + y \in J$, then $-x + x + y \in J$. That is $y \in J$, a contradiction. Conversely if $J \subseteq K$ or $K \subseteq J$, then $J \cup K = K$ or $J \cup K = J$ and hence an ideal.

Note that $\sum_{i \in I} J_i = \langle \cup_{i \in I} J_i \rangle$.

Example:
$R = R[x_1, x_2, \ldots x_n], J = \langle x_1, x_2, \ldots x_n \rangle$, ideal generated by $x_1, x_2, \ldots x_n$.
Then J^m is the set of all polynomials with no terms of degree less than m.

Definition of Comaximal:
Two ideals J, K are said to be *coprime* or *comaximal* if and only if $J + K = R$.
Note that two ideals are coprime if and only if there exist $x \in J$ and $y \in K$ such that $x + y = 1$.

Example:
In $\mathbb{Z}_6$, $\langle 2 \rangle + \langle 3 \rangle = \{0,2,4\} + \{0,3\} = \mathbb{Z}_6$. Therefore the $\langle 2 \rangle$ and $\langle 3 \rangle$ are comaximal in $\mathbb{Z}_6$.

Result:
If J and K are coprime, then $J \cap K = JK$.

Proof:
We have $JK \subseteq J \cap K$
If $J + K = R$ then

$J \cap K = R(J \cap K) = (J + K)(J \cap K)$
$\subseteq JK$
That is $J \cap K = JK$.

Theorem:
Collection of all ideals of a ring forms a complete lattice with respect to inclusion.

Proof:
We have $\langle x_1, \dots, x_n \rangle = \langle \{x_1, \dots, x_n\} \rangle$ and $\langle \emptyset \rangle = \{0\}$.
Put $I(R) = \{J \mid J \; is \; an \; ideal \; of \; R\}$
Here the inclusion in ideals has the following properties. Let $I, J, K \subseteq R$. Then

1. $J \subseteq J$ for any ideal J of R, reflexive.
2. For any $I \neq J$, we have either $I \subseteq J$ or $J \subseteq I$.
3. If $I \subseteq J$ and $J \subseteq K$, then $I \subseteq K$, that is transitive.

So collection of ideals with respect to inclusion is a partially ordered set.
If $S \subseteq I(R)$, then the greatest lower bound of S is intersection of all ideals in S.
That is, $glb \; S = \cap \{J \mid J \in S\}$
and least upper bound of S is ideal generated by union of all ideals in S.
That is $lub \; S = \langle \cup \{J | \; J \in S\} \rangle$.
So $I(R)$ is a complete lattice.

Properties of operations on ideals:
The three operations so far defined (sum, intersection, product) are all commutative and associative.

Result:
Let J and K be two ideals of a ring R, then we get a chain of inclusions as follows:

$$JK \subseteq J \cap K \subseteq J \cup K \subseteq J + K.$$

Proof:
Since J and K are ideals of $R, JK \subseteq J$ and $JK \subseteq K$. That is $JK \subseteq J \cap K$. From set theoretic definitions we have $J \cap K \subseteq J \cup K$. Finally, we can write $J = J + \{0\}$ and $K = \{0\} + K$. So J and K contained in $J + K$. We have already seen that $J + K$ is the smallest ideal contains J and K. Hence $J \cup K \subseteq J + K$.

Example 1:
Put $R = \mathbb{Z}$, $J = \langle m \rangle, K = \langle n \rangle$, where $m, n \in \mathbb{Z}$.
$JK = \langle mn \rangle$
$J \cap K = \langle lcm\{m, n\} \rangle$
$J \cup K = n\mathbb{Z} \cup m\mathbb{Z}$
$J + K = \langle g.c.d\{m, n\} \rangle$
Here
$JK \subset J \cap K \subset J \cup K \subset J + K$.

Example 2:
Consider the ring $\mathbb{Z}_8$ with addition modulo 8 and multiplication modulo 8. Let $J = \langle 2 \rangle$ and $K = \langle 4 \rangle$, then

$JK = \langle 0 \rangle$
$J \cap K = \langle 4 \rangle$
$J \cup K = \langle 2 \rangle$
$J + K = \langle 2 \rangle$
Here
$JK \subset J \cap K \subset J \cup K = J + K.$

Remark:
Let J, K and L be ideals of the ring R, then
(1) $J(K + L) = JK + JL$;
(2) $J \cap (K + L) \supseteq (J \cap K) + (J \cap L)$;
(3) $K \subseteq J$ implies $J \cap (K + L) = (J \cap K) + (J \cap L)$ (the modular law)
(4) $(J + K)(J \cap K) \subseteq JK$.

Example:
Consider the set of integers $\mathbb{Z} = R$ and let $a, b, c \in \mathbb{Z}, J = a\mathbb{Z}, K = b\mathbb{Z}$ and $L = c\mathbb{Z}$. Then
$J \cap (K + L) = a\mathbb{Z} \cap (gcd\{b, c\}\mathbb{Z})$
$= (lcm(a, gc\, d(b, c))\mathbb{Z}$
$= \big(gc\, d\big(lcm(a, b), lcm(a, c)\big)\big)\mathbb{Z}$
$= lcm(a, b)\mathbb{Z} + lcm(a, c)\mathbb{Z}$
$= (J \cap K) + (J \cap L).$
Further
$(J + K)(J \cap K) = (a\mathbb{Z} + b\mathbb{Z})(a\mathbb{Z} \cap b\mathbb{Z})$
$= (gcd(a, b)\,\mathbb{Z})(lcm(a, b)\mathbb{Z})$
$= gcd(a, b)\, lcm(a, b)\mathbb{Z}$
$= ab \cdot \mathbb{Z}$
$= (a\mathbb{Z})(b\mathbb{Z})$
$= JK$

Definition of Direct Product:
Let $R_1, R_2 \ldots R_n$ be rings. Their direct product $R = \prod_{i=1}^{n} R_i$ is the set of all sequences $x = (x_1, \ldots, x_n)$ with $x_i \in R_i (1 \leq i \leq n)$ and componentwise addition and multiplication.

Definition of Projections on product of ideals:
A is a commutative ring with identity element $(1,1, \ldots,1)$We have projections $p_i : R \to R_i$ defined by $p_i(x) = x_i$.

Remark:
Let R be a ring and $J_1, J_2, \ldots, J_n$ ideals of R. Define a homomorphism $\phi : R \to \prod_{i=1}^{n} \frac{R}{J_i}$ by the rule $\phi(x) = (x + J_1, \ldots, x + J_n)$. Then:
(1) If J_i, J_j are coprime whenever $i \neq j$, then $\prod J_i = \cap J_i$.
(2) ϕ is surjective if and only if J_i, J_j are coprime whenever $i \neq j$.
(3) ϕ is injective if and only if $\cap J_i = \Phi$.