Direct sum of rings

The direct sum $R_1 \oplus R_2$ (or direct product $R_1 \times R_2$) of rings R_1 and R_2 is the ring of all ordered pairs (r_1, r_2) where $r_i \in R_i$, with an addition and a multiplication defined by adding and multiplying the "components": $(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$ and $(r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$.

The "projection" subsets $R_1^* = \{(r_1, 0) \mid r_1 \in R_1\}$ and $R_2^* = \{(0, r_2) \mid r_2 \in R_2\}$ are isomorphic to R_1 and R_2, resp.

R_1^* and R_2^* are ideals in $R_1 \oplus R_2$, and every $c \in R_1 \oplus R_2$ has a unique decomposition $c = c_1 + c_2$ with $c_i \in R_i^*$.

Also the converse is true: If I and J are ideals in a ring R such that every $r \in R$ can be uniquely written as $r = i + j$ with $i \in I, j \in J$, then $R \cong I \oplus J$.

$R_1 \oplus R_2/R_1^* \cong R_2$ and $R_1 \oplus R_2/R_2^* \cong R_1$.

Direct sums of more than two rings can be defined and treated analogously.

Direct sum makes possible the construction of rings with various prescribed properties (see e.g. Problems 31, 43, and 48), and in the other direction, it can help to detect the structure of a ring by reducing the problem to the investigation of its direct summands.

Number theory in rings

We assume that R is an integral domain (ID), i.e. a zero-divisor free, commutative ring with identity.

An element dividing every element of R is called a *unit*. Multiplying an element c by a unit, we get an *associate* of c. Associates are equivalent concerning divisibility.

A non-unit (and non-zero) $r \in R$ is *irreducible* if it can be factored **ONLY** trivially: $r = ab \Rightarrow a$ or b is a unit.

A non-unit and non-zero $p \in R$ is a *prime* if it divides a product **ONLY** trivially: $p \mid cd \Rightarrow p \mid a$ or $p \mid b$.

Every prime is irreducible, but the converse is false in many rings.

A greatest common divisor (gcd) of a and b, $\gcd\{a; b\}$ is a common divisor which is a multiple of all common divisors. The definition implies that any two gcds are associates. However, there are many rings where not every pair of elements has a gcd.

The gcd of a and b is closely related to the ideal (a, b) generated by the two elements. Kummer, in trying to prove Fermat's Last Theorem in the middle of the 19th century, introduced the "ideal numbers" just to "substitute" the non-existing gcd and to improve thus the situation due to the lack of unique prime factorization in certain rings.

R is a *unique factorization domain* (UFD) if every non-zero and non-unit element in R is the product of irreducible elements and this decomposition is unique apart from associates and the order of the factors. Recall that $\mathbf{Z}$; $F[x]$ where F is any field; and $\mathbf{Z}[x]$ are UFDs.

R is a UFD iff (i) every irreducible is prime; and (ii) there is no infinite strictly increasing chain of principal ideals.

R is a *principal ideal domain* (PID) if every ideal is a principal ideal. A PID satisfies conditions (i) and (ii), so any PID is a UFD. The converse is false, e.g. $\mathbf{Z}[x]$ is a UFD but not a PID.

R is a *Euclidean domain* (ED) if a *division algorithm* can be performed in R. This means that there is a function $f : R \setminus \{0\} \to \mathbf{N}$ with the following property: To any $b \neq 0, a \in R$ there exist $c, d \in R$ satisfying $a = bc + d$ and $f(d) < f(b)$ or $d = 0$. E.g. $\mathbf{Z}$ and $F[x]$ (where F is a field) are EDs. Another important example is the ring of Gaussian integers to be introduced soon.

Every ED is a PID, hence every ED is a UFD.

The converse is false, e.g. $\{a + b(1 + i\sqrt{19})/2 \mid a, b \in \mathbf{Z}\}$ is a PID, but it is not a ED.