47. Let R_1 and R_2 be arbitrary rings, and consider the set $R_1 \times R_2$ of all ordered pairs (r_1, r_2) where $r_i \in R_i$. We define addition and multiplication on these "vectors" by adding and multiplying the "components": $(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$ and $(r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$. Prove:

(a) We obtain a ring. It is called the *direct sum* $R_1 \oplus R_2$ of R_1 and R_2.

(b) The "projections" $R_1^* = \{(r_1, 0) \mid r_1 \in R_1\}$ and $R_2^* = \{(0, r_2) \mid r_2 \in R_2\}$ satisfy
(b1) $R_i^* \cong R_i$;
(b2) $R_i^* \triangleleft R_1 \oplus R_2$;
(b3) every $c \in R_1 \oplus R_2$ has a unique decomposition $c = c_1 + c_2$ with $c_i \in R_i^*$;
(b4) $R_1 \oplus R_2 / R_1^* \cong R_2$ and $R_1 \oplus R_2 / R_2^* \cong R_1$.

(c) Conditions (b2) and (b3) characterize the direct sum: 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 $R \cong I \oplus J$.

48. Let $R = R_1 \oplus R_2$ where $R_i \neq \{0\}$.

(a) Find zero-divisors in R. This shows that R is *never* a field.

(b) When is R commutative?

(c) When does R have an identity?

(d) Which elements in R have an inverse (if R has an identity)?

49. Which rings have a (non-trivial) direct decomposition:

(a) $\mathbf{C}$; (b) $\mathbf{Z}$; (c) $\mathbf{Z}_9$; (d) $\mathbf{Z}_6$; (e) $\mathbf{R}^{2\times 2}$; (f) the diagonal matrices in $\mathbf{R}^{2\times 2}$.

Number theory in rings

We assume that R is an integral domain (ID), i.e. a zero-divisor free, commutative ring with identity 1.

50. An element dividing every element of R is called a *unit*. Multiplying an element c by a unit, we get an *associate* of c.

(a) The units are exactly the invertible elements of R, i.e. the divisors of 1.

(b) The product and quotient of two units are units again.

(c) What are the units in the following rings:
(c1) $\mathbf{Z}$; (c2) $\mathbf{R}[x]$; (c3) $\mathbf{Z}[x]$; (c4) $D =$ rationals with odd denominators.

(d) There are infinitely many units in the ring $T = \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$.

(e) a and b are associates $\iff$ $a \mid b$ and $b \mid a$ $\iff$ $(a) = (b)$.

51. $r \in R$ is *irreducible* if it is not a unit and $r = ab \Rightarrow a$ or b is a unit. $p \in R$ is a *prime* if it is neither 0, nor a unit, and $p \mid cd \Rightarrow p \mid a$ or $p \mid b$. Prove:

(a) Every prime is irreducible.

(b) The converse is false e.g. in $H = \{a + b\sqrt{10} \mid a, b \in \mathbf{Z}\}$; deduce this from $3 \cdot (-3) = (1 + \sqrt{10})(1 - \sqrt{10})$. To prove that 3 is irreducible, introduce the *norm* of $\alpha = a + b\sqrt{10}$ as $N(\alpha) = (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$ and verify

(b1) $N(\alpha\beta) = N(\alpha)N(\beta)$; and

(b2) α is a unit iff $N(\alpha) = \pm 1$.

(c) In D there is just one irreducible element apart from associates. Why does Euclid's proof about infinitely many primes in $\mathbf{Z}$ fail here?

***52.** R is a *Unique Factorization Domain* (UFD) if every non-zero and non-unit element can be written as the product of irreducible elements and this decomposition is unique apart from associates and the order of the factors (e.g. in $\mathbf{Z}$, we have $12 = 2 \cdot 2 \cdot 3 = (-3) \cdot 2 \cdot (-2)$, etc.). Recall that $\mathbf{Z}$; $F[x]$ where F is any field; and $\mathbf{Z}[x]$ are UFDs. Prove:

(a) D is a UFD, but H is not.

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

(c) If R is a UFD, then $(a) \cap (b)$ is a principal ideal for any $a, b \in R$. Find its generator.

***53.** R is a *principal ideal domain* (PID) if every ideal is a principal ideal. Prove:

(a) In a PID, $d = \gcd\{a, b\} \iff (d) = (a, b)$. What can we say in a general R?

(b) Any PID is a UFD.

(c) The converse of (b) is false, $\mathbf{Z}[x]$ is a counterexample.

54. A ring with a *division algorithm* is called a *Euclidean domain* (ED). 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 $d = 0$. Prove:

(a) $\mathbf{Z}$, $F[x]$, T, and D are EDs.

(b) Every ED is a PID, hence also a UFD.

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

(c) $\mathbf{Z}[x]$ is not a ED.

(d) In a ED, if $f(c)$ is the minimal value of f, then c is a unit.

freud@caesar.elte.hu