All rings are commutative with identity.

**Problem 1.** Show that direct products exist in the category of rings (with identity).

**Definition.** (1) Let $\{a_i\}_{i \in I}$ be ideals in $A$. The ideal $\sum_I a_i$ is defined as

$$\sum_I a_i = \{a_1 + \ldots + a_n \mid a_k \in a_{i_k}\}$$

(2) Let $a_1, \ldots, a_n$ be ideals in $A$. Then $\prod_1^n a_i$ is the ideal generated by all products $(a_1 \ldots a_n)$, $a_i \in a_i$.

One has to check that this actually defines ideals but it is immediate. Note that we could have defined the sum as the ideal generated by all sums of elements from corresponding ideals with the same end result. In (2), though, we did not have an option: if we simply take the set of all products, this is not necessarily an ideal. So we have to consider an ideal generated by all products. Compare this to what happens in groups.

**Problem 2.** Let $a_1, \ldots, a_n$ be ideals in $A$ such that $a_i + a_j = A$ for any $i \neq j$.

(1) Show that there exists $x \in A$ such that

$$x \equiv 1 \pmod{a_1}$$

$$x \equiv 0 \pmod{a_2}$$

$$\ldots$$

$$x \equiv 0 \pmod{a_n}$$

(2) Prove “Chinese remainder theorem”: For any $m_1, \ldots, m_n$ there exists an element $x \in A$ such that

$$x \equiv m_1 \pmod{a_1}$$

$$x \equiv m_2 \pmod{a_2}$$

$$\ldots$$

$$x \equiv m_n \pmod{a_n}$$

Moreover, the residue of $x$ in $A/\prod_1^n a_i$ is uniquely defined.

(3) (This is merely a reformulation in a more ring-theoretic language.) Show that the following are isomorphic:

$$A/(\cap a_i) \simeq A/a_1 \times \cdots \times A/a_n$$

**Definition.** Let $A$ be an integral domain. A Euclidean function on $A$ is a function $\lambda : A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that any $a, b \in A, b \neq 0$ there exist $q, r \in A$ such that $a = bq + r$ and either $r = 0$ or $\lambda(r) < \lambda(b)$. $A$ is a Euclidean domain if it has a Euclidean function associated with it.

(Heuristically, $A$ is a Euclidean domain if $A$ satisfies the Euclidean algorithm.)

**Problem 3.** Prove that a Euclidean domain is a PID.
Corollary. Euclidean domains are UFD.

**Problem 4.** Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ be the ring of Gaussian integers. Here, $i$ is the square root of $-1$. Let
\[
\lambda(a + bi) = N(a + bi) = (a + bi)(a - bi) = a^2 + b^2
\]
(the Norm of $a + bi$).

1. Prove that $\mathbb{Z}[i]$ is factorial.
2. Find the units of $\mathbb{Z}[i]$.
3. Describe all irreducible elements of $\mathbb{Z}[i]$.

**Problem 5.** Let $w = e^{2\pi/3}$ be the third primitive root of unity. Show that $\mathbb{Z}[w] = \{a + bw \mid a, b \in \mathbb{Z}\}$ is Euclidean.

**Problem 6.** Show that the ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is NOT a unique factorization domain.

**Problem 7.** Give an example of an integral domain $A$ and an irreducible element $a \in A$ such that the ideal $(a)$ is not prime.

**Problem 8.** Let $F$ be a field, $F[X]$ be the polynomial ring over $F$, and define $\deg f : F[X] \to \mathbb{Z}_{\geq 0}$ as the degree of the polynomial $f(X)$. Show that $F[X]$ is Euclidean (with respect to the function $\deg$).

**Corollary.** (1). $F[X]$ is a PID.
(2). $F[X]$ is a UFD.

**Remark.** For more than one variable we have that $F[X_1, \ldots, X_n]$ is a UFD but not a PID.

For the next problem, note that by definition a polynomial $f(X) = a_0 + a_1X + \ldots + a_nX^n \in F[X]$ is zero if and only if all coefficients are zero: $a_0 = a_1 = \ldots = a_n = 0$.

**Problem 9.** (a). Let $F$ be a field, and $f(X)$ be a polynomial of degree $n$. Show that $f(X)$ has no more then $n$ roots.
(b). Let $f(X) \in F[X]$. Then $f$ determines a function $f : F \to F$ by evaluation. Assume $F$ is an infinite field. Show that if the function determined by $f$ is zero then $f(X) \equiv 0$ in $F[X]$.
(c). Give a counterexample to the previous statement for a finite field.