6 Rings.

In this section "ring" means commutative associative ring with unity.

◇ **6.1** Prove that in any ring $a0 = 0$ and $-ab = (-a)b$.

Def 6.1 Let R be a ring.
An element $a \in R$ is called *invertible* if $\exists a^{-1} \in R$. The group $R^* = \{a \in R, \quad a \text{ is invertible}\}$ is called *the multiplicative group of R.*
An element $a \in R$, $a \neq 0$ is called *zero divisor* if $\exists b \in R$, $b \neq 0$ such that $ab = 0$.
A ring R is called an *integral domain* if it has no zero divisors.
An element $a \in R$, is called *nilpotent* if $\exists n \in \mathbb{N}$ such that $a^n = 0$.
An element $a \in R$, $a \neq 0, 1$ is called *idempotent* if $a^2 = a$.

◇ **6.2** a) Prove that if a is idempotent then $1 - a$ is idempotent too.
b) Prove that idempotent is a zero divisor.

◇ **6.3** For which $n \in \mathbb{N}$ the ring $\mathbb{Z}_n$ contains a) zero divisors?
b) nilpotent elements ? c) idempotent elements? Suggest an algorithm for finding all idempotent elements in $\mathbb{Z}_n$ for such values of n.

◇ **6.4** Let $A\colon V \to V$ be a linear operator on a vector space V over $\mathbb{C}$. Suppose that A satisfy the equation
a) $A^n = 0$. Find the eigenvalues of A.
b) $A^2 = A$. Find the eigenvalues of A. Prove that V has a basis consisting of the eigenvectors of A. Describe the action of A on V in geometric terms.

◇ **6.5** a) Prove that any ring has a minimal subring isomorphic to Z or Z_n which is generated by $1 \in R$.
b) Prove that if R is an integral domain then its minimal subring is isomorphic either to Z or to Z_p, where p is prime. In this case we say that the *characteristic* $\operatorname{char} R$ of the ring R is either 0 or p.
c) Let R be an integral domain. Prove that if $\operatorname{char} R = p$ then $\forall a \in R$, $a \neq 0$, $\operatorname{ord} a = p$ and if $\operatorname{char} R = 0$ then $\forall a \in R$, $a \neq 0$, $\operatorname{ord} a = \infty$. (Here we mean the order of an element under addition.)

◇ **6.6** a) Prove that if *additive group* of a ring R is a cyclic group generated by 1 then $R \cong \mathbb{Z}_n$ or $R \cong \mathbb{Z}$.
*b) Prove that if *additive group* of a ring R is a cyclic group then it is generated by 1.

◇ **6.7** Find all rings with 4 elements.

◇ **6.8** Prove that any finite integral domain is a field.

Def 6.2 A mapping $f : R \to S$ is called *homomorphism* (of rings with unity) if $\forall x, y \in R$
(1) $f(x + y) = f(x) + f(y)$, (2) $f(x \cdot y) = f(x) \cdot f(y)$ and (3) $f(1) = 1$.
The set $\operatorname{Ker} f = \{x \in R, \ f(x) = 0\} \subset R$ is called *kernel* of f.
The set $\operatorname{Im} f = \{y \in S, \ \exists x \in R \ y = f(x)\} \subset S$ is called *image* of f.

◇ **6.9** Prove that the third condition in definition 6.2 is necessary, i.e. find an example of a mapping f satisfying only first two conditions but not the third one.

◇ **6.10** a) Prove that $\operatorname{Im} f$ is a subring of S.
b) Note that the kernel of a homomorphism $\operatorname{Ker} f$ is not a subring of S, for $1 \notin \operatorname{Ker} f$. Prove that $\operatorname{Ker} f$ is a subgroup of the additive group of the ring R and that $\forall x \in R \ \forall a \in \operatorname{Ker} f \ ax \in \operatorname{Ker} f$.

◇ **6.11** Consider two rings R and S. Define operations on $R \times S$ by $(a, b) + (a', b') = (a + a', b + b')$ and $(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$.
a) Prove that $R \times S$ is a ring.
b) Prove that the mappings $p : R \times S \to R$ and $q : R \times S \to S$ defined by $p(a, b) = a$ and $q(a, b) = b$ are

homomorphisms. Find $\operatorname{Ker} p$ and $\operatorname{Ker} q$.
c) For which m and n $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$?
d) Let R and S have no nilpotent elements. Is it true that $R \times S$ has no nilpotent elements?
e) Let R and S have no idempotent elements. Is it true that $R \times S$ has no idempotent elements? f) Let R and S be integral domains. Is it true that $R \times S$ is an integral domain?
g) Is it true that $(R \times S)^* = R^* \times S^*$?
h) Prove that if $(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$ (φ is the Euler function).

Def 6.3 A subset $I \subset R$ is called an *ideal* if I is a subgroup of R under addition and $\forall x \in R \ \ \forall a \in I \ \ xa \in I$. Note R and $\{0\}$ are ideals of R. Ideals different from R are called *nontrivial* ideals.

$\diamond$ **6.12** a) Find all the ideals of $\mathbb{Z}$ and $\mathbb{Z}_n$.
b) Prove that the kernel of any non-zero homomorphism is a nontrivial ideal.
c) Prove that if an ideal I of a ring R contains an invertible element then $I = R$.

$\diamond$ **6.13** a) Let $a_1, \ldots a_n$ be some non-invertible elements of R. Prove that the set $I = \{x_1a_1 + \ldots + x_na_n, \quad x_i \in R\}$ is an ideal in R. Prove that I is the minimal ideal, containing $a_1, \ldots a_n$. In this case we say that I is *generated* by $a_1, \ldots a_n$ and denoted I by $(a_1, \ldots a_n)$.
b) Prove that every non-invertible element is contained in some nontrivial ideal.
c) Prove that R is a field $\Leftrightarrow$ R has no nonzero nontrivial ideals.
d) Prove that any ideal of $R \times S$ equals to $I \times J$ where I and J are some ideals of R and S.
e) Let $f : R \to S$ be a surjective homomorphism. Prove that the ideals of S are in one-to-one correspondence with the ideals of R containing $\operatorname{Ker} f$.

$\diamond$ **6.14** An ideal generated by one element $a \in R$ is called *principal* ideal and is denoted by (a). If all ideals of an integral ring are principal, the ring is called the *principal* ring.
a) R is a principal ring, $a, b \in R$, $a, b \neq 0$. Then $(a) \subset (b) \Leftrightarrow \exists c \in R$ such that $a = bc$.
b) R is a principal ring, $a, b \in R$, $a, b \neq 0$. Then $(a) = (b) \Leftrightarrow \exists c$ invertible (i.e $c \in R^*$) such that $a = bc$.
c) Prove that the polynomial ring $\mathbb{K}[x] = \{a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, a_i \in \mathbb{K}\}$ is a principal ring. ($\mathbb{K}$ is a field.)
d) Prove that the polynomial ring $\mathbb{K}[x, y]$ is not a principal ring.
e) Is $\mathbb{Z}[x]$ a principal ring?

$\diamond$ **6.15** a) Prove that the set N of all nilpotent elements of a ring R is an ideal of R. N is called the *nil-radical* of R.
b) Find nil-radical of $\mathbb{Z}_n$ for $n = 2, 3, \ldots, 12$.
c) For which n $\mathbb{Z}_n$ has a non-trivial nil-radical?

$\diamond$ **6.16** a) Let I and J be two non-trivial ideals of a ring R. Prove that the sets $I \cap J$, $I \cdot J = \{a_1b_1 + \ldots + a_mb_m, \ a_i \in I, b_i \in J\}$ and $I + J = \{a + b, \ a \in I, b \in J\}$ are ideals in R.
b) Prove that $I \cap J \supset I \cdot J$; find an example when $I \cap J \neq I \cdot J$.
c) Let $I_1 \supset I_2 \supset \ldots \supset I_m \supset \ldots$ be a decreasing sequence of ideals of a ring R. Prove that $\bigcap_{m=1}^{\infty} I_m$ is an ideal. Find an example when $\bigcap_{m=1}^{\infty} I_m = \{0\}$ while all the I_m are nonzero.
d) Let $I_1 \subset I_2 \subset \ldots \subset I_m \subset \ldots$ be an increasing sequences of ideals of a ring R. Prove that $\bigcup_{m=1}^{\infty} I_m$ is an ideal. Prove that if all the I_m are nontrivial then $\bigcap_{m=1}^{\infty} I_m$ is nontrivial too.
e) A nontrivial ideal is called *maximal* if it is not contained in any other nontrivial ideal. Using Zorn lemma prove that maximal ideals exist and that every nontrivial ideal is a subset of a maximal ideal.

$\diamond$ **6.17** Find all the maximal ideals of
a) $\mathbb{Z}$; b) $\mathbb{Z} \times \mathbb{Z}$; c) $\mathbb{Z}_{24}$; d) $\mathbb{C}[x]$; e) $\mathbb{R}[x]$; f) $\mathbb{Z}[x]$.
g) $\mathbb{Z}[\frac{1}{2}] = \{\frac{m}{2^n}, \quad m, n \in \mathbb{Z}, n \geq 0\}$; g) $\mathbb{Z}_{(2)} = \{\frac{m}{n}, \quad m, n \in \mathbb{Z}, (n, 2) = 1\}$.