RINGS, INTEGRAL DOMAINS AND FIELDS

**Definition.** Let $R$ be a set and let $+$ and $\cdot$ be binary operations on $R$. Then $(R, +, \cdot)$ is a ring if

- $(R, +)$ is a commutative group;
- $\cdot$ is a closed associative operation on $R$;
- $\cdot$ is distributive over $+$, i.e., $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$.

**Remark.** The identity element with respect to $+$ is usually denoted by $0$; the inverse of $a$ with respect to $+$ is usually denoted by $-a$. We will often write $ab$ for $a \cdot b$.

**Definition.** Let $(R, +, \cdot)$ be a ring.

- If $\cdot$ is commutative, $R$ is called a commutative ring;
- if there exists an identity element for $\cdot$ (usually denoted by $1$), $R$ is called a ring with unity.

**Theorem.** Let $(R, +, \cdot)$ be a ring and let $a, b, c \in R$. Then

- $a + b = a + c \implies b = c$;
- $0 \cdot a = a \cdot 0 = 0$;
- $(−a) \cdot b = −(a \cdot b)$;
- $(−a) \cdot (−b) = a \cdot b$.

**Invertible elements (units) and divisors of zero**

Let $(R, +, \cdot)$ be a ring with unity $1$ (we shall always assume $1 \neq 0$). Let $u \in R$. In general $u$ may or may not have an inverse with respect to $\cdot$.

**Definition.** We say that $u$ is a unit (or that $u$ is invertible) if $u$ has an inverse with respect to $\cdot$, i.e., if there exists $u' \in R$ such that $u \cdot u' = u' \cdot u = 1$. ($u'$ is usually denoted $u^{-1}$.)
Theorem. If $S$ is a set of all units in $(R, +, \cdot)$, then $(S, \cdot)$ is a group.

Definition. Let $(R, +, \cdot)$ be a ring. If $a, b \in R$, $a \neq 0$, $b \neq 0$, and $a \cdot b = 0$, then $a$ and $b$ are called divisors of zero.

Theorem. Let $(R, +, \cdot)$ be a ring with unity and let $u$ be a unit in $R$. Then $u$ is not a divisor of zero.

Corollary. If $u$ is a divisor of zero, then $u$ is not a unit.

### Integral domains and fields

Integral domains and fields are rings in which the operation $\cdot$ is better behaved.

Definition. Let $(R, +, \cdot)$ be a commutative ring with unity. If there are no divisors of zero in $R$, we say that $R$ is an integral domain (i.e., $R$ is an integral domain if $u \cdot v = 0 \implies u = 0$ or $v = 0$.)

Theorem. Let $(R, +, \cdot)$ be an integral domain. If $ab = ac$ where $a \neq 0$, then $b = c$.

Definition. Let $(R, +, \cdot)$ be a commutative ring with unity. If every element of $R \setminus \{0\}$ is a unit, $R$ is called a field.

Theorem. Let $(R, +, \cdot)$ be a field. Then $(R, +, \cdot)$ is an integral domain.

Corollary. If $(R, +, \cdot)$ is a field, then $(R \setminus \{0\}, \cdot)$ is a commutative group.

Theorem. Let $(R, +, \cdot)$ be a finite integral domain. Then $R$ is a field. (No proof is required.)