DEFINITIONS AND NOTATIONS

Definition 1.1 (operation). For a set $A$, an operation on $A$ is a function $\circ : A \times A \to A$. We usually denote $\circ(a,b)$ by $a \circ b$.

Definition 1.2 (associativity, commutativity). Let $\circ : A \times A \to A$ be an operation on $A$.
- We say that $\circ$ is associative if for any $a,b,c \in A$, we have $(a \circ b) \circ c = a \circ (b \circ c)$.
- We say that $\circ$ is commutative or abelian if for any $a,b \in A$, we have $a \circ b = b \circ a$.

Definition 1.3 (identity, inverse). Let $\circ : A \times A \to A$ be an operation on $A$.
- We say that $e \in A$ is the identity of $(A,\circ)$ if for any $a \in A$ we have $a \circ e = e \circ a = a$.
- If $e \in A$ is the identity of $(A,\circ)$, then for $a,b \in A$ we say that $b$ is an inverse of $a$ if they satisfy $a \circ b = b \circ a = e$.

Definition 3.1 (group). Let $G$ be a set with an operation $\circ : G \times G \to G$. Then $(G,\circ)$ is called a group if
  a) $\circ$ is associative,
  b) the identity element exists in $G$, and
  c) for any $g \in G$, its inverse exists in $G$.

Definition 3.2 (abelian group). A group $(G,\circ)$ is called commutative or abelian if $\circ$ is commutative.

Definition 3.3 (set automorphism group). For a set $A$, define $\text{Aut}_{\text{set}}(A)$ to be the group of bijections $f : A \to A$ whose operation $\circ : \text{Aut}_{\text{set}}(A) \times \text{Aut}_{\text{set}}(A) \to \text{Aut}_{\text{set}}(A)$ is given by composition of functions.

Definition 3.4 (group of integers modulo $n$). For $n \in \mathbb{Z}_{>0}$, $\mathbb{Z}_n$ is defined to be a group \{0,1,2,\ldots,n−1\} whose operation is given by $a \circ b = a + b \pmod{n}$.

Definition 4.1 (subgroup). Let $(G,*)$ be a group and $H \subset G$ be a subset. Then $H$ is said to be a subgroup of $G$ if $(H,* : H \times H \to H)$ is a group.

Definition 4.2 (subgroup generated by a subset). Let $(G,*)$ be a group and $A \subset G$ be a subset. We define $\langle A \rangle$ to be the smallest subgroup of $G$ containing $A$, called the subgroup generated by $A$. Also we say that $\langle A \rangle$ is generated by $A$. 

**Definition 4.3** (cyclic group). A group \((G, \ast)\) is called a **cyclic group** if there exists \(g \in G\) such that \(\langle \{g\} \rangle = G\).

**Definition 5.1** (symmetric group). Let \(A = \{1, 2, \ldots, n\}\) for some \(n \in \mathbb{Z}_{>0}\). Then we define \(S_n\) to be \(\text{Aut}_{\text{set}}(A)\), called the symmetric (or permutation) group on \(n\) elements.

**Definition 5.2** (cycles, transposition). Let \(\alpha \in S_n\).

- \(\alpha\) is called a **cycle** if there exist pairwise different elements \(a_1, a_2, \ldots, a_r \in \{1, 2, \ldots, n\}\) such that \(\alpha(a_1) = a_2, \alpha(a_2) = a_3, \ldots, \alpha(a_{r-1}) = \alpha(a_r), \alpha(a_r) = a_1\), and \(\alpha(b) = b\) if \(b \notin \{a_1, a_2, \ldots, a_r\}\). In this case we usually write \(\alpha = (a_1 \ a_2 \ \cdots \ a_r)\).
- \(\alpha\) is called a **transposition** if \(\alpha = (a \ b)\) for some \(a, b \in \{1, 2, \ldots, n\}\) such that \(a \neq b\).
- \(\alpha\) is called an **adjacent transposition** if \(\alpha = (a \ a + 1)\) for some \(1 \leq a \leq n - 1\).

**Definition 5.3** (notation of permutations). Let \(\alpha \in S_n\).

- The **two-line array notation of** \(\alpha\) is the two-line array \(\begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}\)
- The **cycle notation of** \(\alpha\) is the expression of \(\alpha\) as a product of disjoint cycles.

**Definition 5.4** (even, odd permutation). Let \(\alpha \in S_n\).

- \(\alpha\) is called **even** if it is equal to a product of even number of transpositions.
- \(\alpha\) is called **odd** if it is equal to a product of odd number of transpositions.

**Definition 5.5** (alternating group). Let \(A_nS_n\) be a set of even permutations in \(S_n\). Then \(A_n\) is in fact a subgroup of \(S_n\), called the **alternating group**.

**Definition 6.1** (order). Let \(G\) be a group and \(g \in G\) is an element.

- The **order of** \(G\), denoted \(|G|\), is the cardinal of \(G\).
- The **order of** \(g\), denoted \(\text{ord}(g)\) or \(|g|\), is the smallest \(m \in \mathbb{Z}_{>0}\) such that \(g^m\) is equal to the identity, or \(\infty\) if such \(m\) does not exist.

**Definition 7.1** (homomorphism). Let \(G, H\) be groups. Then a function \(f: G \to H\) is called a **homomorphism** if for any \(a, b \in G\) it satisfies \(f(ab) = f(a)f(b)\).

**Definition 7.2** (kerner, image). Let \(G, H\) be groups and \(f: G \to H\) be a homomorphism.

- The **kernel of** \(f\) is \(f^{-1}(e) \subset G\).
- The **image of** \(f\) is \(f(G) \subset H\).
**Definition 7.3** (various homomorphisms). Let $G, H$ be groups and $f : G \to H$ be a homomorphism.

- $f$ is called a **monomorphism** if $f$ is injective.
- $f$ is called an **epimorphism** if $f$ is surjective.
- $f$ is called an **isomorphism** if $f$ is bijective. If so, we say that $G$ and $H$ are **isomorphic**.
- $f$ is called an **endomorphism** if $G = H$.
- $f$ is called an **automorphism** if $f$ is a bijective endomorphism.

**Definition 7.4** (automorphism group). For a group $G$, define $\text{Aut}(G)$ to be the set of automorphisms of $G$. Then it is naturally a group whose operation is given by composition of functions and called the **group of automorphisms of $G$**.

**Definition 8.1** (equivalence relation). Let $A$ be a set. Then a relation $\sim$ on $A$ is called an **equivalence relation on $A$** if

- for any $a \in A$, $a \sim a$,
- for any $a, b \in A$, if $a \sim b$ then $b \sim a$, and
- for any $a, b, c \in A$, if $a \sim b$ and $b \sim c$ then $a \sim c$.

If $a \sim b$, we say that $a$ is **equivalent to $b$**.

**Definition 8.2** (equivalence class). For a set $A$ with an equivalence relation $\sim$ and for $a \in A$, the set $\{b \in A \mid a \sim b\}$ is called the **equivalence class of $a$**.

**Definition 8.3** (partition). For a set $A$, a **partition of $A$** is a set $P$ consisting of subsets of $A$ such that for any $B, C \in P$, either $B \cap C = \emptyset$ or $B = C$.

**Definition 8.4** (coset). For a group $G$ and its subgroup $H \subset G$, the set $aH$ (resp. $Ha$) for some element $a \in G$ is called the **left (resp. right) coset of $H$ in $G$**.

**Definition 8.5** (coset). For a group $G$ and its subgroup $H \subset G$, the **index of $H$ in $G$** is the cardinal of (left) cosets of $H$ in $G$, denoted $(G : H)$.

**Definition 9.1** (dihedral group). For $n \in \mathbb{Z}_{\geq 2}$, the **dihedral group $D_n$** is the group of isometries of a plane which stabilize a regular $n$-gon.
**Definition 9.2** (quaternion group). The quaternion group $Q_8$ is a group $\{\pm 1, \pm i, \pm j, \pm k\}$ whose operation is given by

\[
\begin{array}{cccccccc}
\circ & 1 & -1 & i & -i & j & -j & k & -k \\
1 & 1 & -1 & i & -i & j & -j & k & -k \\
-1 & -1 & 1 & -i & i & -j & j & -k & k \\
i & i & -i & 1 & -1 & k & -k & -j & j \\
-j & -i & i & 1 & -1 & k & k & j & -j \\
k & k & -k & j & -j & -i & i & -1 & 1 \\
-k & -k & k & -j & j & i & -i & 1 & -1 \\
\end{array}
\]

**Definition 10.1** (normal subgroup). Let $G$ be a group and $H$ is a subgroup of $G$. Then $H$ is called a normal subgroup of $G$ if for any $g \in G$, we have $gHg^{-1} \subseteq H$.

**Definition 10.2** (quotient subgroup). Let $G$ be a group and $H$ is a normal subgroup of $G$. Then $G/H$, the set of left cosets of $H$ in $G$, inherits a natural group structure from $G$ and is called the quotient group (factor group) of $G$ by $H$.

**Definition 11.1** (finitely generated group). A group $G$ is called finitely generated if there exists a finite subset $A \subseteq G$ such that $G = \langle A \rangle$.

**Definition 11.2** ($p$-group). A group $G$ is called a $p$-group for some prime number $p$ if the order of any element in $G$ is a power of $p$.

**Definition 12.1** (group action). Let $G$ be a group and $X$ be a set. Then we say that $G$ acts on $X$, there is an action of $G$ on $X$, or $X$ is a $G$-set, and write $G \curvearrowright X$, if there is a homomorphism $G \to \text{Aut}\set(X)$. In this case, for any $g \in G$ and $x \in X$ we denote by $g \cdot x$ the image of $x$ under the image of $g$ under $G \to \text{Aut}_{\text{set}}(X)$.

**Definition 12.2** (faithful action). Suppose that $G$ acts on $X$. Then we say that $G$ acts faithfully on $X$ if the corresponding homomorphism $G \to \text{Aut}_{\text{set}}(X)$ is injective.

**Definition 12.3** (transitive action). Suppose that $G$ acts on $X$. Then we say that $G$ acts transitively on $X$ if for any $x, y \in X$ there exists $g \in G$ such that $g \cdot x = y$.

**Definition 12.4** (transitive action). Suppose that $G$ acts on $X$. For $x \in X$, the set $\{g \in G \mid g \cdot x = x\}$ is naturally a subgroup of $G$, called the isotropy subgroup (or stabilizer) of $x$. We denote it by $G_x$ or $\text{Stab}_G(x)$.

**Definition 12.5** (fixed point). Suppose that $G$ acts on $X$. For $g \in X$, the set $\{x \in X \mid g \cdot x = x\}$ is called the set of fixed points by $g$, denoted by $X_g$ or $X^g$. 
Definition 12.6 (orbit). Suppose that $G$ acts on $X$.

- For $x \in X$, the set $\{g \cdot x \mid g \in G\}$ is called the orbit of $x$, denoted $G \cdot x$.
- A subset $Y \subset X$ is called an orbit in $X$ under $G$ if $Y = G \cdot x$ for some $x \in X$.
- For $g \in G$, an orbit of $g$ is an orbit of $X$ under $\{g\}$.

Definition 13.1 (ring). Let $A$ be a set with two operations + and ·. Then $(A, +, ·)$ is called a ring (or more precisely a ring with unity) if

- $(A, +)$ is an abelian group,
- · : $A \times A \to A$ is associative,
- for any $a, b, c \in A$, we have $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$, and
- there exists $1 \in A$ such that $1 \cdot a = a \cdot 1 = a$ for any $a \in A$.

We call $1 \in A$ the multiplicative identity of $A$ or the unity of $A$.

Definition 13.2 (zero-divisor, nilpotent element, and unit). Let $A$ be a ring. Then,

- $a \in A$ is called a zero-divisor if $a \neq 0$ and there exists $b \in A$ such that $b \neq 0$ and either $ab = 0$ or $ba = 0$.
- $a \in A$ is called a nilpotent element if $a^n = 0$ for some $n \in \mathbb{Z}_{>0}$.
- $a \in A$ is called a unit if there exists $b \in A$ such that $ab = ba = 1$. We denote by $A^\times$ the subset of $A$ consisting of all units of $A$.

Definition 13.3 (commutative ring, integral domain, and field). Let $A$ be a ring. Then,

- $A$ is called a commutative ring if · : $A \times A \to A$ is commutative.
- $A$ is called an integral domain if $A$ is commutative and $A$ does not contain any zero-divisor.
- $A$ is called a field if $A$ is commutative and $A^\times = A - \{0\}$.

Definition 13.4 (module). Let $(A, +, ·)$ be a ring and $(M, +)$ be an abelian group. Then $M$ is called an $A$-module if there exists a map · : $A \times M \to M : (a, m) \mapsto a \cdot m$ such that

- for any $a \in A$ and $m, n \in M$, we have $a \cdot (m + n) = a \cdot m + a \cdot n$,
- for any $a, b \in A$ and $m \in M$, we have $(a + b) \cdot m = a \cdot m + b \cdot m$,
- for any $a, b \in A$ and $m \in M$, we have $(a \cdot b) \cdot m = a \cdot (b \cdot m)$, and
- for any $m \in M$, we have $1 \cdot m = m$.

Definition 13.5 (vector space). Let $M$ be an $A$-module. Then $M$ is called an $A$-vector space if $A$ is a field.
Definition 13.6 (algebra). Let $A$ be a commutative ring and $B$ is a ring. Then $B$ is called an $A$-algebra if $B$ is an $A$-module and for any $a \in A$ and $x, y \in B$ we have $a \cdot (x \cdot y) = (a \cdot x) \cdot y = x \cdot (a \cdot y)$.

Definition 14.1 (subobject).
\begin{itemize}
  \item Let $A$ be a ring. Then a subset $B \subset A$ is called a subring of $A$ if $B$ is a ring with respect to $+$ and $\cdot$ inherited from $A$ and $B$ contains the unity of $A$.
  \item Let $A$ be a ring and $M$ be an $A$-module. Then a subset $N \subset M$ is called an $A$-submodule of $M$ if $N$ is an $A$-module with respect to $+$ and scalar multiplication inherited from $M$.
  \item Let $A$ be a commutative ring and $B$ is an $A$-algebra. Then a subset $C \subset B$ is called an $A$-subalgebra of $B$ if $C$ is both a subring and an $A$-submodule of $B$.
\end{itemize}

Definition 14.2 (homomorphism).
\begin{itemize}
  \item Let $A$ and $B$ be rings. Then a function $f : A \to B$ is called a ring homomorphism if $f(1) = 1$ and for any $x, y \in A$ we have $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$.
  \item Let $A$ be a ring and $M, N$ be $A$-modules. Then a function $f : M \to N$ is called an $A$-module homomorphism if for any $a \in A$ and $x, y \in M$ we have $f(x + y) = f(x) + f(y)$ and $f(ax) = af(x)$.
  \item Let $A$ be a commutative ring and $B, C$ be $A$-algebras. Then a function $f : B \to C$ is called an $A$-algebra homomorphism if $f$ is both a ring homomorphism and an $A$-module homomorphism.
\end{itemize}

Definition 14.3 (center of a ring). Let $A$ be a ring. Then the center of $A$, denoted $Z(A)$, is defined to be $Z(A) := \{ a \in A \mid ab = ba \text{ for any } b \in A \}$.

Definition 14.4 (ideal). Let $A$ be a ring. Then a subset $I \subset A$ is called an ideal of $A$ if $(I, +)$ is an abelian subgroup of $(A, +)$ and “$I$ absorbs products in $A$,” i.e. for any $x \in I$ and $a \in A$ we have $ax, xa \in I$.

Definition 14.5 (quotient).
\begin{itemize}
  \item Let $A$ be a ring and $I$ be an ideal of $A$. Then $A/I$ is called the quotient of $A$ by $I$. Its ring structure is defined such that $A \to A/I : a \mapsto a + I$ is a ring homomorphism.
  \item Let $A$ be a ring, $M$ be an $A$-module, and $N \subset M$ be an $A$-submodule of $M$. Then $M/N$ is called the quotient of $M$ by $N$. Its $A$-module structure is defined such that $M \to M/N : m \mapsto m + N$ is an $A$-module homomorphism.
\end{itemize}

Definition 14.6 (ideal generated by a subset, principal ideal). Let $A$ be a ring.
\begin{itemize}
  \item For a subset $S \subset A$, we call $(S)$ the ideal of $A$ generated by $S$, defined to be the smallest ideal of $A$ containing $S$.
\end{itemize}
• If $I$ is an ideal of $A$ generated by a single element, then we say that $I$ is a principal ideal.

**Definition 14.7** (module generated by a subset, cyclic submodule). Let $A$ be a ring and $M$ be an $A$-module.

• For a subset $S \subset M$, we call $\langle S \rangle$ the $A$-submodule of $M$ generated by $S$, defined to be the smallest $A$-submodule of $M$ containing $S$.

• If $N$ is an $A$-submodule of $M$ generated by a single element, then we say that $N$ is cyclic.

**Definition 14.8** (prime and maximal ideal). Let $A$ be a commutative ring and $I \subset A$ be an ideal of $A$.

• $I$ is called a **prime ideal of $A$** if for any $a,b \in A$, if $ab \in I$ then either $a \in I$ or $b \in I$.

• $I$ is called a **maximal ideal of $A$** if $I \neq A$ and any ideal of $A$ containing $I$ is equal to either $I$ or $A$.

**Definition 15.1** (finite dimensional vector space). Let $F$ be a field and $V$ be an $F$-vector space. Then $V$ is called finite-dimensional (or finitely generated) if $V = \langle S \rangle$ for some finite subset $S \subset V$ as an $F$-vector space.

**Definition 16.1** (Euclidean domain). Let $A$ be an integral domain. Then $A$ is called an Euclidean domain (abbreviated **ED**) if there exists a function $d : A - \{0\} \to \mathbb{N}$ such that

• $d(a) \leq d(ab)$ for any $a,b \in A - \{0\}$ and

• for any $a \in A$ and $b \in A - \{0\}$, there exists $q,r \in A$ such that $a = bq + r$ and either $r = 0$ or $d(r) < d(b)$.

**Definition 16.2** (Principal ideal domain). Let $A$ be an integral domain. Then $A$ is called a principal ideal domain (abbreviated **PID**) if every ideal of $A$ is principal.

**Definition 16.3** (prime and irreducible element). Let $A$ be an integral domain.

• $p \in A$ is called a **prime element of $A$** if $p \neq 0, p \not\in A^\times$ and $\langle p \rangle$ is a prime ideal of $A$, i.e. if $p|ab$ for some $a,b \in A$, then either $p|a$ or $p|b$.

• $p \in A$ is called an **irreducible element of $A$** if $p \neq 0, p \not\in A^\times$ and if $p = ab$ for some $a,b \in A$ then either $a \in A^\times$ or $b \in A^\times$.

**Definition 16.4** (unique factorization domain). Let $A$ be an integral domain. Then $A$ is called a unique factorization domain (abbreviated **UFD**) if

• for any $a \in A$ such that $a \neq 0$, there exists $u \in A^\times$, $r \in \mathbb{N}$, and irreducible elements $p_1,p_2,\ldots,p_r$ such that $a = up_1p_2\cdots p_r$, and
• if \( up_1p_2 \cdots p_r = vq_1q_2 \cdots q_s \) for some \( u, v \in A^\times, \ r, s \in \mathbb{N}, \) and irreducible elements \( p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s \in A, \) then \( r = s \) and one can reorder \( q_1, q_2, \ldots, q_s \) such that \( p_i = u_iq_i \) for some \( u_i \in A^\times \) for \( 1 \leq i \leq r = s. \)