Algebra Definitions

On Rings, Polynomials, and Fields

1 Section 16.1 - Rings

1. A **ring** R is a set that is closed under two binary operations, $+$ and $\times$. The following conditions must also be satisfied:
   (a) Additive commutativity.
   (b) Additive associativity.
   (c) Additive identity.
   (d) Additive inverse.
   (e) Multiplicative associativity.
   (f) Multiplicative distributivity 1 & 2.
2. A **ring with unity (or with identity)** is a ring R that has multiplicative identity.
3. A **commutative ring** is a ring R that has multiplicative commutativity.
4. An **integral domain** is a commutative ring R with identity such that for all $a, b \in R$ $ab = 0$ implies $a = 0$ or $b = 0$.
5. A **division ring** is a ring R that has multiplicative inverse for all nonzero $a \in R$.
6. A **zero divisor** of a commutative ring R is an $a \in R$ $(a \neq 0)$ such that there exists a nonzero $b \in R$ such that $ab = 0$.
7. The **ring of quaternions** is the set $\mathbb{H} = \{a+b\hat{i}+c\hat{j}+d\hat{k} \mid a, b, c, d \in \mathbb{R}\}$, where $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \hat{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \hat{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \hat{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

2 Section 16.2 - Integral Domains and Fields

1. A **field** is a commutative division ring.

2. The **characteristic** of a ring R is the least positive integer n such that $nr = 0$ for all $r \in R$. If no such n exists, the characteristic of R is defined to be 0. (denote the characteristic of R by char$R$).

3 Section 16.3 - Ring Homomorphisms and Ideals

1. A **ring homomorphism** is a map $\phi : R \to S$ (where R, S are rings) such that $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.

2. A **ring isomorphism** is a bijective map $\phi : R \to S$ where R, S are rings.

3. The **kernel** of a ring homomorphism $\phi : R \to S$ is the set $\ker \phi := \{r \in R \mid \phi(r) = 0\}$.

4. An **evaluation homomorphism** is a ring homomorphism of the form $\phi_\alpha : C[a, b] \to \mathbb{R}$ or other such related homomorphisms.

5. An **ideal** of a ring R is a subring I such that if $a \in I$ and $r \in R$, then $ar, ra \in I$.

6. The **trivial ideals** of a ring R are the subrings $\{0\}$ and R.

7. A **principal ideal** of a commutative ring R (with identity) is an ideal of the form $\langle a \rangle = \{ar \mid r \in R\}$.

8. A **two-sided ideal** I is a subring of a ring R such that $rI \subset I$ and $Ir \subset I$ for all $r \in R$.

9. A **one-sided ideal** I is a subring of a ring R is one such that $rI \subset I$ for all $r \in R$ (a **left ideal**) or $Ir \subset I$ for all $r \in R$ (a **right ideal**).

4 Section 17.1 - Polynomial Rings

1. A **polynomial over** R is an expression of the form $f(x = \sum_{i=0}^{n} a_i x^i)$ with **indeterminate** x. Define $a_0, \ldots, a_n$ to be the **coefficients** of f and a_n is the **leading coefficient** of f. A polynomial is **monic** if its leading coefficient a_n is 1. The **degree** (write: $\deg f(x) = n$) is the largest nonnegative number for which $a_n \neq 0$. If no such n exists, then $f = 0$, the **zero polynomial** and define the degree of $f = 0$ to be $-\infty$. Denote $R[x]$ to be the set of all polynomials with coefficients in a ring R.

2. $R[x, y]$ is the **ring of polynomials in two indeterminates** x, y **with coefficients in** R. $R[x_1, \ldots, x_n]$ is the **ring of polynomials in** n **indeterminates with coefficients in** R.

5 Section 17.2 - The Division Algorithm

1. Let $p(x) \in F[x]$ and $\alpha \in F$. Then α is a **zero** (or **root**) of $p(x)$ if $p(x) \in \ker \phi_\alpha$, where ϕ_α is an evaluation homomorphism. In other words, α is a zero of $p(x)$ if $p(\alpha) = 0$.

2. Let F be a field. A monic polynomial $d(x)$ is a **greatest common divisor** of $p(x), q(x) \in F[x]$ if $d(x) \mid p(x)$ and $d(x) \mid q(x)$; and, for any other polynomial $d'(x)$ that divides both $p(x)$ and $q(x)$, $d'(x) \mid d(x)$. (write: $d(x) = \gcd(p(x), q(x))$). Two polynomials $p(x), q(x)$ are **relatively prime** if $\gcd(p(x), q(x)) = 1$.

6 Section 17.3 - Irreducible Polynomials

1. A nonconstant polynomial $f(x) \in F[x]$ is **irreducible** over a field F if $f(x)$ cannot be expressed as a product of two polynomials $g(x), h(x) \in F[x]$, where $\deg g(x), \deg h(x) < \deg f(x)$.

7 Section 3.1 - Integer Equivalence Classes & Symmetries

1. A **symmetry** of a geometric figure is a rearrangement of the figure preserving the arrangement of its sides and vertices as well as its distances and angles.

2. A map from the plane to itself preserving the symmetry of an object is called a **rigid motion**.

3. A **permutation** of a set S is a bijective map $\pi : S \to S$.

8 Section 3.2 - Definitions & Examples

1. A **binary operation** or **law of composition** on a set G is a function $G \times G \to G$ that assigns to each pair $(a, b) \in G \times G$ a unique element $a \circ b$, or $ab \in G$, called the composition of a and b.

2. A **group** $(G, \circ)$ is a set G together with a binary operation $(a, b) \mapsto a \circ b$ that satisfies the following axioms (where $a, b, c \in G$):

   (a) Associativity ($(a \circ b) \circ c = a \circ (b \circ c)$).

   (b) Identity ($\exists e \in G$ such that $e \circ a = a \circ e = a$).

   (c) Inverse ($\forall a \in G \exists a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$).

3. A group G with the property that $a \circ b = b \circ a$ (for all $a, b \in G$) is called **abelian** or **commutative**. Groups not satisfying this property are said to be **nonabelian** or **noncommutative**.

4. Let $U(n) := \mathbb{Z}_n \setminus \{0\}$. Then, $U(n)$ is called the **group of units** of $\mathbb{Z}_n$.

5. We have the following:

   (a) $\mathbb{C}^\star = \{z \in \mathbb{C} : z \neq 0\}$ is the **multiplicative group of complex numbers**.

   (b) $\mathbb{M}_2(\mathbb{R}) = \{$2x2 matrices of real entries$\}$.

   (c) $GL_2(\mathbb{R}) = \{$2x2 invertible matrices of real entries$\}$ is the **general linear group**.

(d) $GL_2(\mathbb{R}) \subsetneq \mathbb{M}_2(\mathbb{R})$.

6. Let $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. Then, the set $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$ is called the **quaternion group**.

7. A group G is **finite** (or has **finite order**) if it contains a finite number of elements. Otherwise, the group is said to be **infinite** (or has **infinite order**). The **order** of a finite group is the number of elements that it contains.

9 Section 3.3 - Subgroups

1. Let G be a group. H is a **subgroup** of G if H is a subset of G such that when the group operation of G is restricted to H, then H is a group on its own right.

2. The subgroup $H = \{e\}$ of a group G is called the **trivial group**. A subgroup that is a proper subset of G is called a **proper subgroup**.

3. $SL_2(\mathbb{R})$ is the **special linear group** and we have the following definitions: $SL_2(\mathbb{R}) = \{$2x2 matrices of real entries and determinant 1$\}$.

10 Section 4.1 - Cyclic Subgroups

1. Let G be a group and $a \in G$. Let $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$. Then, $\langle a \rangle$ is called the **cyclic subgroup** generated by a. If G contains some element a such that $G = \langle a \rangle$, then G is a **cyclic group** and call a the **generator** of G. If $a \in G$, define the **order** of a to be the smallest $n \in \mathbb{Z}_{>0}$ such that $a^n = e$, and write $|a| = n$. If there is not such integer n, we say that the order of a is infinite and write $|a| = \infty$.

11 Section 4.2 - Multiplicative Group of Complex Numbers

1. The **circle group** is defined to be $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$.

2. The complex numbers satisfying the equation $z^n = 1$ are called the **nth roots of unity**.

3. A generator for the group of n^{th} roots of unity is called a **primitive nth root of unity**.

12 Section 5.1 - Definitions & Notation (Permutation Groups)

1. The **symmetric group** on n letters is the group of permutations on a finite set $X = \{1, \dots, n\}$.

2. A subgroup of S_n is called a **permutation group**.

3. A permutation $\sigma \in S_X$ is a **cycle of length *k*** if there exist elements $a_1, \dots, a_k$ in X such that $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_k) = a_1$ and $\sigma(x) = x$ for all other $x \in X$.