MATH20212 Cheat Sheet

1 Rings

A **ring** is a set R and two binary operations, written $+$ and $\times$, on R which satisfies the following conditions:
(R1) $\langle R, +\rangle$ is an abelian group with identity 0
(R2) $\times$ is associative
(R3) $\times$ is distributive over $+$
(R4) there exists an element $1 \in R$, different from 0, that is an identity for $\times$

Let R be a ring and $S \subseteq R$. Then S is a **subring** of R if it is a ring in its own right with respect to the same addition and multiplication as in R and S contains 1_R.

Subring Test: Let R be a ring and $S \subseteq R$, then S is a subring of R, iff:
$(i)\, 1 \in S$
$(ii)\, r + s, r \times s \in S$, for all $r, s \in S$
$(iii)\, -r \in S$ for all $r \in S$

Let R be a ring. The **ring of polynomials** $R[X]$ in the indeterminate X is defined as follows:
Elements: formal linear combinations of the form $\sum_{i\geq 0} a_i X^i$ with $a_i \in R$ for $i = 0, 1, \ldots$
Equality: $\sum_{i\geq 0} a_i X^i = \sum_{i\geq 0} b_i X^i \iff a_i = b_i$ for all $i \geq 0$
Addition: $\sum_{i\geq 0} a_i X^i + \sum_{i\geq 0} b_i X^i = \sum_{i\geq 0} (a_i + b_i) X^i$
Multiplication: $(\sum_{i\geq 0} a_i X^i)(\sum_{i\geq 0} b_i X^i) = \sum_{k\geq 0} (\sum_{i+j=k} a_i b_j) X^k$
Zero element is $\sum_{i\geq 0} 0X^i = 0$ and the **one** is $1X^0 + \sum_{i\geq 1} 0X^i = 1$

For a polynomial $f = \sum_{i\geq 0} a_i X^i$, we define the **degree** of f, denoted $deg(f)$, to be the largest i such that $a_i \neq 0$ and we let $deg(f) = -\infty$ if $f = 0$.

2 Integral Domains and Fields

The **characteristic**, $char(R)$, of a ring R is the least positive integer n such that $n \cdot 1 = 0$. If there is no such n, then the characteristic of R is defined to be 0.

A non-zero element $r \in R$ is a **zero-divisor** if there is a non-zero element $s \in R$ with $rs = 0$ or $sr = 0$.

The ring R is a **domain** if, for all $r, s \in R$, $rs = 0 \implies r = 0$ or $s = 0$, so a domain is a ring with **no** zero-divisors. A commutative domain is called an **integral domain**.

A **division ring** is a ring in which every non-zero element has a right inverse and a left inverse. In this case, these inverses are the same. We write r^{-1} for this **inverse** of r and say that r is **invertible** or that r is a **unit**. A **field** is a commutative division ring.

An element r of a ring R is **nilpotent** if there is some integer $n \geq 1$ with $r^n = 0$ and the least such n is the **index of nilpotence** of r. An element $r \in R$ is **idempotent** if $r^2 = r$ - and 0 and 1 are idempotent in any ring.

3 Isomorphisms, Homomorphisms and Ideals

If R and S are rings then an **isomorphism** from R to S is a **bijection** $\theta : R \to S$ such that, for all $r, r' \in R$:

$$\theta(r + r') = \theta(r) + \theta(r') \quad \text{and} \quad \theta(r \times r') = \theta(r) \times \theta(r')$$

If θ is an isomorphism from R to S, then we write $\theta : R \simeq S$. We say that R and S are **isomorphic**, and write $R \simeq S$, if there is an isomorphism from R to S.

If R and S are rings then a **homomorphism** from R to S is a map $\theta : R \to S$ such that, for all $r, r' \in R$:

$$\theta(r + r') = \theta(r) + \theta(r') \quad and \quad \theta(r \times r') = \theta(r) \times \theta(r') \quad and \quad \theta(1_R) = 1_S$$

An **embedding**, or **monomorphism**, is an injective homomorphism.

If $\theta : R \to S$ is a homomorphism of rings then the **kernel** of θ, $ker(\theta)$, is the set $\{r \in R \,|\, \theta(r) = 0\}$.

An **automorphism** of a ring is an isomorphism from the ring to itself.

An **ideal** of a ring R is a subset $I \subseteq R$ such that:

$$0 \in I \quad \text{and} \quad a + b \in I, \text{ for all } a, b \in I \quad \text{and} \quad ar \in I \text{ and } ra \in I \text{ for all } a \in I \text{ and for all } r \in R$$

We write $I \triangleleft R$ to mean that I is an ideal of R.

If $a \in R$ then $\{r_1 a s_1 + \cdots + r_n a s_n \mid n \geq 1, r_i, s_i \in R\}$ is an ideal which contains a and is the smallest ideal of R containing a. It is called the **principal ideal generated by** a and is denoted $\langle a \rangle$. If R is commutative, then its description simplifies: $\langle a \rangle = \{ar \mid r \in R\}$. A **principal** ideal is one which can be generated by a single element.

In every ring $\langle 0 \rangle = \{0\}$ is the smallest ideal and is called the **trivial ideal**.
In every ring $\langle 1 \rangle = R$ is the largest ideal and every other ideal is referred to as a **proper ideal**.

The more general notion of **right ideal** is defined as for ideal but with the third condition replaced by the weaker condition: $a \in I$ and $r \in R$ implies $ar \in I$. Then, if $a \in R$, the **principal right ideal generated by** $a \in R$ is defined to be the set $\{ar \mid r \in R\}$ and is denoted aR.