

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 $i = 0, 1, \dots$

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 $\sum_{i \geq 0} 0 X^i = 0$ and the **one** is $1X^0 + \sum_{i \geq 1} 0 X^i = 1$

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 $f = 0$.

Lemma 1.3 Let R be a ring. Then, for all $a, b \in R$, $0a = a0 = 0$, $a(-b) = (-a)b = -(ab)$ and $(-a)(-b) = ab$.

2 Integral Domains and Fields

The **characteristic**, $\text{char}(R)$, 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.

Lemma 2.2 If $\text{char}(R) = n > 0$, then $n \cdot r = 0$ for every $r \in R$ and if m is a positive integer then $m \cdot 1 = 0 \iff n \mid m$

Proposition 2.7 Suppose that R is a domain, then the polynomial ring $R[X]$ is a domain.

Corollary 2.8 Suppose that R is a domain. Then the ring, $R[X_1, \dots, X_n]$, of polynomials in n indeterminates with coefficients in R , is a domain.

Lemma 2.10 If R is a ring and $r \in R$ has both a right and a left inverse, then these are equal and unique.

Lemma 2.12 For $n \geq 2$: \mathbb{Z}_n is a integral domain $\iff \mathbb{Z}_n$ is a field $\iff n$ is a prime.

Proposition 2.14 Every division ring is a domain. Every field is an integral domain.

Lemma 2.16 In any ring R , the set of units R^* forms a group under multiplication.

3 Isomorphisms, Homomorphisms and Ideals

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

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

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

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

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 $\{r_1as_1 + \cdots + r_nas_n \mid n \geq 1, r_i, s_i \in R\}$ 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 .

4 Factor Rings

Let R be a ring and let I be a proper ideal. Let R/I denote the set of cosets of I in the additive group $\langle R, + \rangle$, $R/I = \{r + I \mid r \in R\}$ with operations $+$ and \times defined on R/I as follows:

$$(r + I) + (s + I) = (r + s) + I \quad \text{and} \quad (r + I) \times (s + I) = (r \times s) + I$$

This ring is the **factor ring** (or **quotient ring**) of R by I .

Fundamental Isomorphism Theorem Let I be a proper ideal of the ring R .

(i) the map $\pi : R \rightarrow R/I$ defined by $\pi(r) = r + I$ is a surjective ring homomorphism with kernel I . π is called the **canonical surjection** or **canonical projection**.

(ii) if $\theta : R \rightarrow S$ is a homomorphism and $I \subseteq \ker(\theta)$ then there is a unique map $\theta' : R/I \rightarrow S$ with $\theta' \circ \pi = \theta$. This map θ' is a homomorphism.

(iii) the map θ' is injective iff $\ker(\theta) = I$. If θ is surjective and $\ker(\theta) = I$ then θ' is an isomorphism.

Some other theorem Let I be an ideal of the ring R , then there is a natural, inclusion-preserving, bijection between the set of ideals of R which contain I and the set of ideals of the factor ring R/I :

- to an ideal $J \geq I$ there corresponds $\pi J = \{r + I \mid r \in J\} = \{\pi(r) \mid r \in J\}$, an ideal in R/I
- to an ideal $K \triangleleft R/I$ there corresponds $\pi^{-1}K = \{r \in R \mid \pi(r) \in K\}$, an ideal in R

The notation J/I is also used instead of πJ for the image of J in R/I .

An ideal I of a ring R is **maximal** if it is proper and for any ideal J with $I \leq J \leq R$, then either $J = I$ or $J = R$.

Another theorem If $I \leq J$ are ideals of R , so J/I is an ideal of R/I , then $(R/I)/(J/I) \simeq R/J$.

A proper ideal I of a commutative ring R is **prime** if whenever $r, s \in R$ and $rs \in I$ then either $r \in I$ or $s \in I$.

5 Polynomial Rings and Factorisation

Division Theorem for Polynomials Let K be a field and take $f, g \in K[X]$ with $g \neq 0$, then there are (unique) $q, r \in K[X]$ with $f = qg + r$ and $\deg(r) < \deg(g)$ or $r = 0$. We say q is the **quotient** and r is the **remainder** when f is divided by g .

An element $a \in K$ is a **root** (or **zero**) of $f \in K[X]$ if $f(a) = 0$.

The **greatest common divisor** (or **highest common factor**) of polynomials f, g is a polynomial d such that d divides f and g and, if h is any polynomial dividing both f and g , then h divides d . Write $d = \gcd(f, g)$. This polynomial is defined only up to a non-zero scalar multiple so, if we want a unique gcd then we can insist that d has to be **monic** (ie. coefficient of highest power of X is equal to 1).

An element $r \in R$ is **irreducible** if r is not invertible and if, whenever $r = st$ either s or t is invertible.

Elements $r, s \in R$ are **associated** if $s = ur$ for some invertible element $u \in R$.

A commutative domain R is said to be a **Unique Factorisation Domain (UFD)**, if every non-zero, non-invertible element of R has a unique factorisation as a product of irreducible elements. *Uniqueness* here means up to rearrangement of factors and associated factors.

A **Principal Ideal Domain (PID)** is a commutative domain in which every ideal is principal.

6 Constructing Roots for Polynomials

Kronecker's Theorem Let K be a field and let $f \in K[X]$ be irreducible of degree n . Define $L = K[X]/\langle f \rangle$, then:
(i) L is a field and the canonical homomorphism $\pi : K[X] \rightarrow K[X]/\langle f \rangle$ induces an embedding $\theta : K \rightarrow L$
(ii) $\alpha = \pi(X) \in L$ is a root of f
(iii) the dimension of L as a vector space over K is n , with $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ being a basis of L over K , so every element of L has a unique representation of the form $a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0$ with $a_{n-1}, \dots, a_1, a_0 \in K$ (note that we have identified K with its image $\theta(K)$ in L .)