MATH367 Cheat Sheet

Oğul Can Yurdakul

Last Updated: 17/01/2021

Contents

1 Groups

Group: A non-empty set G with a binary operation $\cdot : G \times G \to G$ is a group if

(G1) For all $x, y, z \in G$, $x(yz) = (xy)z$.

(G2) There exists $e \in G$ such that for all $g \in G$ $eg = ge = g$, called the identity of the group.

(G3) For all $x \in G$, there exists $y \in G$ such that $xy = yx = e$, i.e. each element has an inverse in the group.

The order of a group G is the cardinality of its domain, denoted $o(G) = |G|$.

A group is called abelian if the group operation is commutative, i.e. for all $x, y \in G$, $xy = yx$.

Some immediate lemmas are as follows:

1. e, the identity element, is unique.
2. The inverse x^{-1} for each x is unique.
3. $(x^{-1})^{-1} = x$
4. $(xy)^{-1} = y^{-1}x^{-1}$
5. $e^{-1} = e$
6. $xx = x \Rightarrow x = e$
7. Cancellation laws: $xy = xz \Rightarrow y = z$ and $yx = zx \Rightarrow y = z$.

Subgroup: Let G be a group and $H \subset G$. If H is also a group under the same operation as G, H is called a subgroup of G, denoted $H \leq G$.

A subgroup H necessarily has the same identity and inverse per its elements as the parent group G.

A non-empty subset $H \subset G$ is a subgroup if and only if for all $x, y \in G$, $xy^{-1} \in H$.

Generated Subgroup: Let $S \subset G$ for some group G. Define

$$\mathcal{S} = \{H : H \leq G, S \subset H\}$$

Then $\langle S \rangle = \bigcap_{H \in \mathcal{S}} H$ is the subgroup generated by S.

$$\langle S \rangle = \{s_1^{e_1} ... s_n^{e_n} : s_i \in S, e_i = \pm 1, i = 1, ..., n, n \in \mathbb{Z}^+\}$$

If $G = \langle S \rangle$, then S is called a set of generators for G.

If $S = \{a\}, a \in G$, then we write $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

Cyclic Group: A group G is called cyclic if there is a single element generating it, i.e. $G = \langle a \rangle$ for some $a \in G$. A cyclic group may have more than one generator.

Every cyclic group is abelian, but the converse is generally not true, i.e. not every abelian group is cyclic.

If $G = \langle a \rangle$ is of finite order with $|G| = n$, then $e = a^n$ and $n = \min\{k \in \mathbb{Z}^+ : e = a^k\}$.

If $G = \langle a \rangle$ is of infinite order, then $a^j = e$ if and only if $j = 0$, meaning $a^j \neq e$ for all $j \in \mathbb{Z} - \{0\}$. Further, $a^j = a^i$ if and only if $j = i$.

$|HK|$: For H, K finite subgroups of G, we have

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Order of an Element: For $a \in G$, the order is defined as $o(a) = o(\langle a \rangle)$. Regarding the order of an element, the followings are equivalent:

⇳ a) $o(a) = n$.

⇳ b) $a^n = e$ and $n = \min\{k \in \mathbb{Z}^+ : e = a^k\}$.

⇳ c) $a^n = e$ and $n|m$ for any $m \in \mathbb{Z}$ with $a^m = e$.

A finite group of order n is cyclic if and only if it contains an element g with $o(g) = n$.

Every subgroup of a cyclic group is cyclic. If $G = \langle g \rangle$ and $|G| = m > 1$, then a proper subgroup $H \leq G$ is given by $H = \langle g^k \rangle$ for some $k \in \mathbb{Z}$ with $k|m$ and $k > 1$. In this case, $o(H)|m$.

The order of an element $a^k \in G$ is given by

$$o(a^k) = \frac{o(a)}{\gcd(k, |G|)}$$

Coset: Let $H \leq G$ and $a \in G$. Then the sets

$$aH = \{ah : h \in H\}$$
$$Ha = \{ha : h \in H\}$$

are respectively the left and right cosets of H in G, and a is their representative.

$aH = bH$ if and only if $b^{-1}a \in H$ or equivalently $a^{-1}b \in H$. Similarly, $Ha = Hb$ if and only if $ba^{-1} \in H$ or equivalently $ab^{-1} \in H$.

The above statement implies that $aH = H$ if and only if $a \in H$ or equivalently $a^{-1} \in H$. (Take $b = e$.)

There are as many distinct right cosets of H as distinct left cosets of H.

For all $a \in G$, $|H| = |Ha| = |aH|$.

All the right/left cosets of some H are disjoint, unless they are equal. Since their union gives the whole of G, the right/left cosets of H partition G.

Index: Let $H \leq G$. Then the number of distinct right/left cosets of H in G is called the index of H in G, denoted $[G : H]$.

$[G : H] = 1$ if and only if $G = H$.

Lagrange's Theorem: Let $H \leq G$. Then

$$|G| = [G : H]|H|$$

In particular if G is finite, then

$$|H| \big| |G|$$

Take a group of finite prime order and take one of its non-trivial cyclic groups. Then as this subgroup is non-trivial, it has index larger than 1, and consequently must equal to the order of the whole group as the group is of prime order and the order of any subgroup must divide the group order. Therefore the whole group turns out to be cyclic, and therefore cyclic. In short, any finite group of prime order is abelian.

If G is a finite group and $a \in G$, then $o(a)|o(G)$.

If G is a finite abelian group of order $|G|$ and p is a prime dividing $|G|$, then G has an element of order p, and hence a subgroup of order p.

Normal Subgroup: Let $H \leq G$. Then if any of the below equivalent conditions are satisfied, H is said to be a normal subgroup, denoted $H \trianglelefteq G$:

$\Updownarrow$ a) $aH = Ha$ for all $a \in G$.

$\Updownarrow$ b) $aHa^{-1} = H$ for all $a \in G$.

$\Updownarrow$ c) $a^{-1}Ha = H$ for all $a \in G$.

$\Updownarrow$ d) $aHa^{-1} \subseteq H$ for all $a \in G$.

$\Updownarrow$ e) $aha^{-1} \in H$ for all $a \in G$ and $h \in H$.

If G is abelian, then every subgroup is normal.

$\langle e \rangle = \{e\}$ and G are (trivial) normal subgroups of G.

$\mathcal{Z}(G)$, the center of G, is a normal subgroup.

$$h \in \mathcal{Z}(G) \iff \forall g \in G hg = gh$$

A group G is called simple if $G \neq \{e\}$ and the only normal subgroups of G are G and $\{e\}$.

Any subgroup of index 2 is normal.

Quotient Group: Let $H \trianglelefteq G$. Then the set of all right/left cosets of H, denoted G/H, forms a group under the following operation:

$$(aH)(bH) = (ab)H \quad \forall aH, bH \in G/H$$

$|G/H| = [G : H]$. If further G is finite, then $|G/H| = \frac{||G|}{|H|}$.

If G is abelian, then so is G/H.

If G is cyclic, then so is G/H.,

A quotient group of a non-abelian group can turn out to be abelian.

Every subgroup of G/N is of the form H/N for some subgroup $H \leq G$ containing N.

If $N \trianglelefteq H$, $N \trianglelefteq G$ and $N \leq H \leq G$, then $H/N \leq G/N$.

If $N \trianglelefteq H \leq G$, then $H/N \trianglelefteq G/N \iff H \trianglelefteq G$.

Homomorphism: Let $\alpha : G \to H$ be a function between groups. If $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, n \in G$, then α is called a group homomorphism. Further, it is called a

monomorphism if α is injective (one-to-one),

epimorphism if α is surjective (onto),

isomorphism if α is bijective, in which case we write $G \simeq H$ to say that G is isomorphic to H,

endomorphism if $H = G$, i.e. $\alpha : G \to G$

automorphism if $\alpha : G \to G$ and α is bijective.

We also make the following definitions for a homomorphism:

Image: $\mathrm{Im}(\alpha) = \{h \in H : \exists g \in G, h = \alpha(g)\}$

Kernel: $\ker(\alpha) = \{g \in G : \alpha(g) = e_H\}$

The following facts then hold for a group homomorphism:

1. $\alpha(e_G) = e_H$
2. $\alpha(a^{-1}) = \alpha(a)^{-1}$
3. $\alpha(a^n) = \alpha(a)^n$
4. If $o(a) = n$, then $o(\alpha(n))|n$. In particular, $o(\alpha(a)) \leq o(a)$, so if $o(\alpha(a)) = \infty$, then $o(a) = \infty$.
5. If $G' \leq G$, then $\alpha(G') \leq H$.
6. If $H' \leq H$, then $\alpha^{-1}(H') \leq G$. If further $H' \trianglelefteq H$, then $\alpha^{-1}(H') \trianglelefteq G$.
7. If G is abelian, then so is $\alpha(G)$.
8. If α is an epimorphism, i.e. it is surjective, then the image of $G' \trianglelefteq G$ is also normal in H, i.e. $\alpha(G') \trianglelefteq H$.
9. Composition of homomorphisms is again a homomorphism.
10. $\mathrm{Im}(\alpha) \leq H$ and $\ker(\alpha) \trianglelefteq G$.

For an isomorphism $\alpha : G \to H$, the followings hold:

1. $\alpha^{-1} : H \to G$ is an isomorphism.
2. G is abelian if and only if H is abelian.
3. For all $a \in G$, $o(a) = o(\alpha(a))$.
4. G is cyclic if and only if H is cyclic.

Every finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +)$ and every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$. (Map to their exponent!)

Fundamental Theorem of Homomorphisms: Let $\alpha : G \to H$ be a group homomorphism and $g : G \to {}^{G}/_{\ker \alpha}$ ve the natural (canonical) homomorphism:

$$\begin{aligned} g : \ & G \to {}^{G}/_{\ker \alpha} \\ & a \mapsto g(\ker \alpha) \end{aligned}$$

Then there is a injective homomorphism $\psi : {}^{G}/_{\ker \alpha} \to H$ such that $\alpha = \psi \circ g$:

$$\begin{aligned} \psi : \ & {}^{G}/_{\ker \alpha} \to H \\ & g(\ker \alpha) \mapsto \alpha(g) \end{aligned}$$

Isomorphism Theorems: Let $\alpha : G \to H$ be a group homomorphism.

Ist Isomorphism Theorem: Then

$${}^{G}/_{\ker \alpha} \simeq \mathrm{Im}(G)$$

IInd Isomorphism Theorem: (Moving $\cdot$ to $\cap$) Let $H \leq G$, $K \trianglelefteq G$. Then

1) $H \cap K = \{hk : h \in H, k \in K\} \trianglelefteq H$
2) $K \trianglelefteq HK$
3) $H/H\cap K \simeq HK/K$

IIIrd Isomorphism Theorem: (Quotient group cancellation) Let $H, K \trianglelefteq G$ and $H \leq K$. Then we have $K \trianglelefteq H$ and $K/H \trianglelefteq G/H$ as well, and further

$$G/H/K/H \simeq G/K$$

Group Action: Let G be a group and S be any non-empty set. An action (left action) of G on S is defined as a function

$$\begin{aligned} \bullet : \ & G \times S \to S \\ & (g, s) \mapsto g \bullet s \end{aligned}$$

satisfying the given two properties:

1) $g_1 \bullet g_2 \bullet s = (g_1 g_2) \bullet s$ for all $g_1, g_2 \in G$ and $s \in S$.
2) $e \bullet s = s$ for all $s \in S$.

We make the following definitions for a group action:

Orbit: Define an equivalence relation $\sim$ as follows:

$$a \sim b \iff g \bullet a = b \text{ for some } g \in G$$

The equivalence classes of $\sim$ are called as the orbits of G on S, denoted by $[a]$ or $\mathrm{Orb}(a)$ for $a \in S$.

Stabilizer: For all $a \in S$, the stabilizer of a or the isotropy group of a, denoted G_a or $\mathrm{Stab}(a)$, is given by

$$G_a = \{g \in G : g \bullet a = a\}$$

Stabilizers are subgroups of G.

Orbit-Stabilizer Theorem: Let G act on S. For all $a \in S$,

$$[G : G_a] = |[a]|$$

and if further G is finite, then

$$|[a]| = \frac{|G|}{[G : G_a]}$$

A result for finite S is

$$|S| = \sum_{a \in A \subset S} [G : G_a]$$

where A contains a single representative from each orbit.

Actions as Permutations: Let G act on $S \neq \varnothing$. Then this action induces a homomorphism from G onto $\mathcal{A}(S)$, where $\mathcal{A}(S)$ is the group of all permutations of S, given by

$$\begin{aligned} \varphi : G &\to \mathcal{A}(S) \\ g &\mapsto \mathcal{T}_g(a) \ : S \to S \\ & \qquad\qquad a \mapsto g \bullet a \end{aligned}$$

Extended Cayley's Theorem: Let $H \leq G$, $S = \{aH : a \in G\}$. Then there exists a homomorphism ψ from G so $\mathcal{A}(S)$ such that $\ker \psi \subseteq H$.

External Direct Product: Let G_i be a family of groups for some finite set of indices $I_n \ni i$. Then $G = \prod G_i$ is a group with respect to the binary operation given by

$$(g_1, g_2, ..., g_n)(h_1, h_2, ..., h_n) = (g_1h_1, g_2h_2, ..., g_nh_n)$$

$H_i = \{(e_1, ..., a_i, ..., e_n) : a_i \in G_i\}$ are normal subgroups of G.

All $g \in G$ can be expressed as $g = h_1h_2...h_n$ where $h_i \in H_i$.

$H_i \cap (H_1...H_{i-1}H_{i+1}...H_n) = \{e_G\}$ for all i.

$G = H_1...H_n$

Internal Direct Product: Let G be a group and $N_i : i \in I_n$ be a finite family of normal subgroups of G with some index set I_n. Then G is called the internal direct product of $N_1, ..., N_n$ if every $g \in G$ can be uniquely expressed as $a = a_1a_2...a_n$ where $a_i \in N_i$.

$G = N_1N_2...N_n$

$N_i \cap (N_1...N_{i-1}N_{i+1}...N_n) = \{e_G\}$

$N_i \cap N_j = \{e_G\}$ whenever $i \neq j$. Consequently, $a_ia_j = a_ja_i$ for $a_i \in N_i$, $a_j \in N_j$ whenever $i \neq j$.

$G \simeq \prod_{i \in I_n} N_i = N_1 \times N_2 \times ... \times N_n$ under $\alpha : a = a_1a_2...a_n \mapsto (a_1, a_2, ..., a_n)$

$o(g_1, ..., g_n) = \text{lcm}(o(g_1), ..., o(g_n))$

Cyclic & Product Groups Theorem: Let G and H be finite cyclic groups. Then $G \times H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

A corollary to this theorem is that if G is a finite cyclic group and $|G| = mn$ where m and n are relatively prime, then $G \simeq \mathbb{Z}_n \times \mathbb{Z}_m$.

Fundamental Theorem of Finite Abelian Groups: Every finite abelian group is (isomorphic to) a direct product of cyclic groups of prime power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

Conjugation: Let $a, b \in G$. We say that a and b are conjugates in G if there exists some $g \in G$ such that $gbg^{-1} = a$.

Notice that with the conjugation definition in mind, we can reinterpret the definition of normal subgroups. A normal subgroup is a subgroup which is closed under conjugation, i.e. if $H \leq G$ is normal, then any conjugate aha^{-1} for any $a \in G$ is contained in H for all $h \in H$.

Conjugation Action: Let G act on *itself* by conjugation:

$$\begin{aligned} \bullet : \ & G \times G \to G \\ & (g, a) \mapsto g \bullet a = gag^{-1} \end{aligned}$$

Conjugacy Classes: (Orbits) The orbit of $a \in G$ under the conjugation action is called the conjugacy class of a, denoted $[a]$ or $\text{Cl}(a)$:

$$[a] = \{gag^{-1} : g \in G\}$$

If G is abelian,$[a] = \{a\}$ as for all $g \in G$ we have $ga = ag \iff gag^{-1} = a$.

Centralizer: (Stabilizers) Let $H \leq G$ and H act on G by conjugation:

$$\begin{aligned} \bullet : \ & H \times G \to G \\ & (h, g) \mapsto h \bullet g = hgh^{-1} \end{aligned}$$

The stabilizer of $a \in G$ under the conjugation action is called the centralizer of a in H, written

$$C_H(a) = \{h \in H : hah^{-1} = a\} = \{h \in H : ha = ah\}$$

If $G = H$, i.e. G is acting on itself via conjugation, then it is simply called the centralizer of a, written

$$C_G(a) = \{g \in G : gag^{-1} = a\} = \{g \in G : ga = ag\}$$

Notice that the centralizer, i.e. the stabilizer under the conjugation action, of some element $g \in G$ gives the set of elements in some $H \leq G$ that commute with g.

Normalizer: (Stabilizer of subgroups) Now let $H \leq G$ act on the set $\mathcal{S}$ of all subgroups of G:

$$\begin{aligned} \bullet : \ & H \times \mathcal{S} \to \mathcal{S} \\ & (h, K) \mapsto h \bullet K = hKh^{-1} = \{hkh^{-1} : k \in K\} \end{aligned}$$

Then the stabilizer of K in H is called the normalizer of K in H, written

$$N_H(K) = \{h \in H : hKh^{-1} = K\} = \{h \in H : hK = Kh\}$$

If $G = H$, it is simply called the normalizer of K:

$$N_G(K) = \{g \in G : gKg^{-1} = K\} = \{g \in G : gK = Kg\}$$

$N_G(K)$ is the largest set in which K is normal, i.e.

1. $K \trianglelefteq N_G(K)$ and
2. $K \trianglelefteq G$ if and only if $N_G(K) = G$.

Orbit-Stabilizer Theorem for Conjugation Action: Let G be a finite group. Then

The number of elements in $C_G(x)$ for any x is $[G : C_G(x)]$, which divides $|G|$:

$$|[x]| = [G : C_G(x)] \big| |G|$$

If $[x_1], ..., [x_n]$ are are all of the conjugacy classes of G, then

$$|G| = \sum_{i=1}^{n} |[x_i]| = \sum_{i=1}^{n} [G : C_G(x_i)]$$

The number of subgroups of G conjugate to K is $[G : N_G(K)] = |[K]|$.

Class Equation: Recall that if $a \in \mathcal{Z}(G)$, i.e. commutes with every element in G, then $[a] = \{a\}$, since $gag^{-1} = a \iff ga = ag$ for all $g \in G$. Therefore we can separate the members of $\mathcal{Z}(G)$ out from the class equation above to obtain

$$|G| = |\mathcal{Z}(G)| + \sum_{i=1}^{m} |[x_i]| = |\mathcal{Z}(G)| + \sum_{i=1}^{m} [G : C_G(x_i)] \qquad \text{(Class Equation)}$$

where x_i's are elements not in $\mathcal{Z}(G)$ coming from different conjugacy classes.

Subgroup of Prime Order of Finite Abelian Groups: Let G be a finite abelian group of order n and p be a prime dividing n. Then G contains an element of order p, and hence has a subgroup of order p.

Cauchy Theorem: (above but not abelian) Let G be a finite group, not necessarily abelian, of order n and p be a prime dividing n. Then G contains an element of order p, and hence has a subgroup of order p.

Subgroup of Any Order of Finite Abelian Groups: Let G be a finite group of order n and m be a positive integer dividing n. Then G has a subgroup of order m.

***p*-groups:** Let p be a prime. A group G is called a p-group if the order of each element of G is a power of p. A subgroup H of a group is called a p-subgroup if H is a p-group.

A non-trivial group G is a p-group if and only if $|G| = p^k$ for some $k \in \mathbb{Z}^+$.

Let G be a p-group. Then $\mathcal{Z}(G) \neq \{e\}$.

A group of order p^2 for any prime p is abelian.

Sylow *p*-subgroup: Let G be a finite group of order $n = p^k m$ where p is a prime *not* dividing m, i.e. p^k is the highest power of p in the prime decomposition of n. A subgroup of G of order p^k is called a Sylow p-subgroup.

Sylow Theorems:

Ist Sylow Theorem: (Existence) Let G be a finite group of order $n = p^k m$, where p is prime, $k, m \in \mathbb{Z}^+$ and p and m are relatively prime. Then

(i) G has a subgroup of order p^k for all $0 \leq r \leq k$.

(ii) For each k with $1 \leq r \leq k-1$, a subgroup of order p^r is a normal subgroup of a subgroup of order p^{r+1}, so, in short:

$$\{e\} = P_0 \trianglelefteq P_1 \trianglelefteq P_2 \trianglelefteq ... \trianglelefteq P_k, |P_r| = p^r$$

IInd Sylow Theorem: (Relation) Let G be a finite group and let P_1, P_2 be two Sylow p-subgroups. Then P_1 and P_2 are conjugates, i.e. there exists some $g \in G$ such that $gP_1g^{-1} = P_2$.

IIIrd Sylow Theorem: (Number) Let G be a finite group and let n_p denote the number of Sylow p-subgroups of G. Then

(i) $n_p \equiv 1 \pmod{p}$

(ii) If $|G| = p^k m$, p prime, $m \in \mathbb{Z}^+$ and $p \nmid m$, then $n_p | m$.

(iii) If P is any Sylow p-subgroup of G, then by the Orbit-Stabilizer Theorem for conjugation action,

$$n_p = [G : N_G(P)] = |[P]|$$

where $N_G(P)$ is the normalizer of P.

$n_p = 1$ for some Sylow p-subgroup P in and only if $P \trianglelefteq G$.

If G is abelian, all subgroups of G are normal, therefore there is exactly one Sylow p-subgroup for each p dividing $|G|$.

Sylow p-subgroups for different primes can only have trivial intersection.

2 Rings

Ring: Let R be a non-empty set and $+$ and $\cdot$ be two binary operations on R. Then $(R, +, \cdot)$ is called a ring if

(R1) $(R, +)$ is an abelian group.

(R2) $\cdot$ is associative.

(R3) For all $a, b, c \in R$, we have $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

The additive identity of R is denoted as 0_R and is called the zero of the ring. For all $a \in R$, $0_R a = a0_R = 0_R$. A ring R is called commutative if $\cdot$ is commutative.

A ring R is called a ring with identity/unity if it has a multiplicative identity, denoted 1_R. If it exists, it is unique.

For a ring R with identity, a non-zero element is called a unit if it has a multiplicative inverse. For a unit, its multiplicative inverse is unique. If R^* denotes all units of R a ring with identity, then R^* is non-empty ($1_R \in R^*$) and if $a, b \in R^*$, then $ab \in R^*$. Therefore R^* is a group under $\cdot$.

For a ring, the expected identities hold:

- $0_R a = a0_R = 0_R$.
- $-ab = (-a)b = a(-b)$ and $(-a)(-b) = ab$.
- $a(b - c) = ab - ac$ and $(a - b)c = ac - bc$.

Zero Divisor: Let $a \neq 0_R$. Then a is called a zero divisor if there exists $b \neq 0_R$ such that $ab = 0_R$.

Integral Domain: A commutative ring with unity without zero divisors is called an integral domain.

Division Ring: A ring (not necessarily commutative) with unity is called a division ring if every element is a unit. Naturally, every division ring is a ring without zero divisors.

Field: A commutative division ring is called a field.

Being commutative, a field is therefore an integral domain.

It can be shown that every element in a finite integral domain has a multiplicative inverse, hence making it a field. In short, every finite integral domain is a field.

Cancellation Equivalences: Let R be a ring. Then the followings are equivalent:

⇳ a) If $a, b \in R$ and $ab = 0_R$, then $a = 0_R$ or $b = 0_R$. (i.e. R has no zero divisors)

⇳ b) If $a, b \in R$ and $x \neq 0_R$, then $ax = bx$ (or equivalently $(a - b)x = 0_R$) implies $a = b$ for all $0_R \neq x$ in R.

⇳ c) If $a, b \in R$ and $x \neq 0_R$, then $xa = xb$ (or equivalently $x(a - b) = 0_R$) implies $a = b$ for all $0_R \neq x$ in R.

Characteristic: The characteristic of a ring R, denoted $\text{char}(R)$, is the least positive integer n such that $nx = 0_R$ for all $x \in R$, i.e. it is the order of the underlying additive abelian group. If no such integer exists, then we say that R has characteristic zero.

An infinite ring can have non-zero characteristic.

The characteristic of an integral domain R is either 0 or a prime.

Subring: Let R be a ring and $S \subseteq R$. S is called a subring of R if S itself is a ring under the same operations of R.

A subring of R is never empty as it always contains 0_R.

$S \subseteq R$ is a ring if and only if

1. $S \neq \varnothing$
2. $x - y \in S$ for all $x, y \in S$, so it is an additive subgroup of R.
3. $xy \in S$ for all $x, y \in R$, so it is closed under multiplication.

A subring with identity may have an identity different than the identity of the whole ring.

Ideal: (Normal subgroup analogue) Let R be a ring and $I \subseteq R$ be a subring. Then I is called

a left ideal if $\forall r \in R$, $\forall i \in I$, $ri \in I$.

a right ideal if $\forall r \in R$, $\forall i \in I$, $ir \in I$.

a (two-sided) ideal if $\forall r \in R$, $\forall i \in I$, $ri, ir \in I$.

A subset $I \subseteq R$ is an ideal if and only if

1. $I \neq \varnothing$
2. $x - y \in I$ for all $x, y \in S$, so it is an additive subgroup of R.
3. $ri, ir \in I$ for all $r \in R$ and for all $i \in I$, so it is closed under multiplication *and* it is an ideal.

The only ideals of a division ring D are $\{0_D\}$ and D itself.

As every field is a (commutative) division ring by definition, the same goes for fields: The only ideals of a field F are $\{0_F\}$ and F itself.

For an ideal I of R the followings hold:

- $1_R \in I \iff I = R$
- $I \neq R \iff I$ contains no units of R.

Ring Homomorphism: Let R and S be two rings. A function $\alpha : R \to S$ satisfying

$$\forall a, b \in R \ \alpha(a + b) = \alpha(a) + \alpha(b)$$

$$\forall a, b \in R \ \alpha(ab) = \alpha(a)\alpha(b)$$

is called a ring homomorphism. Then the following properties hold:

1) For any $r \in R$ and $n \in \mathbb{Z}^+$, $\alpha(nr) = n\alpha(r)$ and $\alpha(r^n) = \alpha(r)^n$.
2) For A a subring of R, $\alpha(A)$ is a subring of S.
3) If A is further an ideal and α is onto, then $\alpha(A)$ is an ideal of S.
4) For B and ideal of S, $\alpha^{-1}(B)$ is an ideal of R.
5) If R is commutative, then so is $\alpha(R)$.
6) If R has unity 1_R, $S \neq \{0_S\}$ and α is onto, then $\alpha(1_R) = 1_S$. If both R and S have unity, $\alpha(1_R)$ need not be 1_S unless S is an integral domain or α is onto.

Kernel is defined with respect to the additive identity as

$$\ker \alpha = \{r \in R | \alpha(r) = 0_S\}$$

$\ker \alpha$ is an ideal of R.

Factor Ring: (Quotient group analogue) Let R be a ring and I be an ideal of R. The factor ring R/I is defined as follows:

$$R/I = \{r + I | r \in R\}$$

which is the quotient group with respect to the underlying abelian additive group of R. The operations on the factor ring are defined as follows:

$$(r + I) + (s + I) := (r + s) + I$$

$$(r + I)(s + I) := (rs) + I$$

If R is commutative, so is R/I.
If R has unity 1_R, R/I has unity $1_R + I$.
$\alpha : r \to r + I$ is called as the canonical homomorphism from R to R/I, with $\ker \alpha = I$.

Isomorphism Theorems: Let $\alpha : R \to S$ be a ring homomorphism.

I. Isomorphism Theorem: (Usual stuff) Then

$$R/\ker \alpha \simeq \text{Im}(\alpha) = \alpha(R)$$

II. Isomorphism Theorem: (Moving + to $\cap$) Let R be a ring, S a subring of R and I an ideal of R. Then

1) $S + I = \{s + i | s \in S, i \in I\}$ is a subring of R and I is an ideal of $S + I$.
2) $S \cap I$ is an ideal of S.
3) $S+I/I \simeq S/S\cap I$

III. Isomorphism Theorem: (Factor ring cancellation) Let R be a ring and I and J be ideals of R with $J \subset I$, and J an ideal of I. Then I/J is an ideal of R/J with

$$R/J/I/J \simeq R/I$$

Notice that these isomorphism theorems are the exact analogues of the isomorphism theorems for groups. We have just taken the underlying additive abelian group of each ring and replaced the term 'normal subgroup' with 'ideal'.

Principal Ideal: (Cyclic group analogy) Let R be a ring and $a \in R$. Then

$$Ra = \{ra | r \in R\}$$

is a left ideal of R, called a principal left ideal of R. A principal right ideal aR is defined similarly.

Let R be a commutative ring with identity. An ideal I of R is called principal if there is some $a \in R$ that generates I, meaning

$$I = aR = Ra = (a)$$

Every ideal of $\mathbb{Z}$ is principal.

Maximal Ideal: Let R be a ring. An ideal $M \neq R$ of R is called maximal whenever for any ideal I of R with $M \subset I \subseteq R$, we have either $M = I$ or $I = R$.

Let R be a commutative ring with identity and let M be an ideal of R. Then M is maximal if and only if R/M is a field, so the followings are equivalent:

⇳ a) R is a field.
⇳ b) R has no non-trivial ideals.

$\Updownarrow$ c) $\{0_R\}$ is a maximal ideal of R.

Prime Ideal: Let R be a commutative ring. Then an ideal P of R is a prime ideal of R if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$ for all $a, b \in R$.

Let R be a commutative ring with unity. Then R/P is an integral domain if and only if P is a prime ideal of R.

For R a commutative ring with identity, every maximal ideal of R is also a prime ideal of R.

Polynomial Rings: Let R be a commutative ring with identity. Then

$$R[x] = \{a_0 + ... + a_n x^n | n \geq 0, a_i \in R\}$$

is called as the polynomial ring over R.

If R is commutative, then so is $R[x]$.

If R has identity, so does $R[x]$.

If R has no zero divisors, then $R[x]$ has no zero divisors.

If R is an integral domain, then so is $R[x]$.

If F is a field, then $F[x]$ is an integral domain.

Degree: Let R be a commutative ring with identity, and $R[x]$ the polynomial ring over R. For all non-zero polynomials $f \in R[x]$, the degree of f is defined as follows:

$$\deg(f) = n \iff f(x) = a_0 + ... + a_n x^n, a_n \neq 0$$

For R a polynomial ring and $f, g \in R[x]$, we have

$$\deg(fg) = \deg(f) + \deg(g)$$

Monic Polynomial: Let R be a commutative ring with identity. For $f(x) = a_0 + ... + a_n x^n \in R[x], a_n \neq 0$, the leading coefficient is defined to be a_n. If we have $a_n = 1_R$, then f is said to be a monic polynomial.

Units in $F[x]$: For a field F, the only units in $F[x]$ are the non-zero constant polynomials. No polynomial of positive degree ($\deg \geq 1$) can have an inverse in $F[x]$, hence $F[x]$ is not a field.

Division Algorithm for Polynomials: Let F be a field and let $f, g \in F[x]$ with $g \neq 0$. Then there are polynomials $q, r \in F[x]$ satisfying

$$f = qg + r$$

where either $r = 0$ or $\deg(r) < \deg(g)$. The polynomials q, called the quotient, and r, called the remainder, are uniquely determined for each $0 \neq g, f \in F[x]$.

Root/Zero: Let F be a field and $f(x) \in F[x]$. For all $r \in F$, define $f(r)$ as expected. If for some $r \in F$ we have $f(r) = 0_F$, we call r a root or a zero of $f(x)$.

Remainder Theorem: Let R be a commutative ring with identity. For all $f \in F[x]$ and $a \in F$, there exists some $g(x) \in F[x]$ such that

$$f(x) = (x - a)g(x) + f(a)$$

For $f \in F[x]$ and $a \in F$, $(x - a)$ divides $f(x)$ if and only if a is a root of f.

PID: An integral domain R is a Principal Ideal Domain (PID) if every ideal I in R is a principal ideal, meaning there exists some $a \in R$ such that $I = (a) = aR$.

Divisibility & Associates: Let R be an integral domain and let $a, b \in R$. We say that b divides a, denoted $b|a$, if there exists some $c \in R$ such that $a = bc$. ($0_R|0_r$ is allowed.) If further this c is a unit (i.e. has a multiplicative inverse), then we say that b is an associate of a, denoted $a \sim b$. The following properties then hold:

1) $a \sim a$
2) $a \sim b \Rightarrow b \sim a$
3) $a \sim b \wedge b \sim c \Rightarrow a \sim c$ *(1-3 make $\sim$ an equivalence relation)*
4) $\in R$ $a|a$
5) $a|b \wedge b|a \Rightarrow a \sim b$
6) $a|b \wedge b|c \Rightarrow a|c$
7) $b|a \Rightarrow (a) \subset (b)$
8) $a \sim b \iff (a) = (b)$ *(use 7)*
9) b is a proper divisor of $a \iff aR \subsetneq bR \subsetneq R$ or equivalently $(a) \subsetneq (b) \subsetneq R$
10) $u \in R$ is a unit $\iff u \sim 1 \iff uR = (u) = R \iff u|1_R$

Proper Divisor: Let R be an integral domain and let $a, b \in R$. Then b is said to be a proper divisor of a if $b|a$ and b is neither a unit nor an associate of a, i.e.

a) $b|a$
b) b is not a unit
c) $b \not\sim a$

Irreducibility: Let R be an integral domain. An element $q \in R$ is said to be irreducible if $q \neq 0$, q is not a unit and q has no proper divisors, i.e. $q = ab$ implies either a or b is a unit.

Any associate of an irreducible element is also irreducible.

Gauss Lemma: Suppose that $f \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ is a monic polynomial of positive degree. Then f is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$.

2nd and 3rd Degree Polynomials: Let F be a field and let $f \in F[x]$ be a polynomial of degree 2 or 3. Then f is irreducible over F if and only if F has no roots in F.

Candidate Rational Roots: Let $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$ be of degree n and $a_0 \neq 0$. Let $u/v \in \mathbb{Q}$ be a root of $f(x)$ where u and v are relatively prime. Then $u|a_0$ and $v|a_n$.

Linear Test: Let F be a field and $0 \neq a, b \in F$. Then $f(x) \in F[x]$ is irreducible if and only if $f(ax + b) \in F[x]$ is irreducible.

Reduction mod p / Mod p Test: Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of positive degree and p be a prime integer. Set $f_p(x) \in \mathbb{Z}_p[x]$ to be the reduction of f modulo p, i.e. take the coefficient modulo p. If $f_p \in \mathbb{Z}_p[x]$ is irreducible, then $f \in \mathbb{Z}$ is irreducible. The converse need not be true!

Eisenstein's Criterion: Let $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$. If there exists a prime integer p such that

a) $p \mid a_i$ for $i = 0, \ldots, n-1$
b) $p \nmid a_n$

c) $p^2 \nmid a_0$

then f is irreducible in $\mathbb{Q}$.

Maximality in a PID: Let R be a PID and let $I \neq \{0_R\}$ be an ideal of R. Then I is maximal if and only if the generator of I is irreducible, i.e. $I = (p)$ where p is irreducible.

Prime Element: Let R be a commutative ring with identity and $p \in R$, $p \neq 0$, and p not a unit. Then p is a prime element of R if

$$p|ab \Rightarrow p|a \vee p|b$$

In any integral domain, a prime element is irreducible.

If further we are in a PID, every irreducible element is also a prime element. Therefore in a PID, an element p is irreducible if and only if it p is a prime element.

In a commutative ring with identity R, $p \in R$ is a prime element if and only if pR is a non-zero prime ideal in R.

If further we are in a PID, an ideal is maximal if and only if it is a prime ideal.

Equivalent Factorizations: Let R be an integral domain, $0 \neq a \in R$ and a not a unit. Two factorizations

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_k$$

where p_i and q_j are irreducible elements are said to be equivalent if $n = k$ and there is a one-to-one correspondence between the factors p_i and q_j such that corresponding factors are associates.

UFD: An integral domain R is called a Unique Factorization Domain (UFD) if every non-zero, non-unit element $a \in R$ may be represented as a product of irreducible elements in R and any two such representations of an element $a \in R$ are equivalent.

Every PID is a UFD.

If F is a field, then the polynomial domain $F[x]$ is a UFD.

If A is a UFD, then so is $A[x]$.

If A is a UFD, then every irreducible element $a \in A$ is prime. Then as every prime element is irreducible in all integral domains, in a UFD, an element $a \in A$ is prime if and only if it is irreducible.

Euclidean Domains: Let A be an integral domain and let $\delta : A - \{0_A\} \to \mathbb{Z}^+ \cup \{0\}$ be a function such that

1) For all $a, b \in A - \{0_A\}$, if $b|a$ then $\delta(b) < \delta(a)$. Equivalently for all $a, b \in A - \{0_A\}$, $\delta(a) \leq \delta(ab)$.
2) For all $a, b \in A - \{0_A\}$ with $b \neq 0_A$, there exists $q, r \in A$ such that $a = bq + r$ where either $r = 0$ or $\delta(r) < \delta(b)$.

Then δ is called a Euclidean norm or valuation on A. The integral domain A forms a Euclidean domain (ED) with respect to the Euclidean norm δ.

Every Euclidean domain is a PID, so we have the following picture:

$$\textbf{ED} \Rightarrow \textbf{PID} \Rightarrow \textbf{UFD}$$

Let R be a ED and $0 \neq a \in R$. Then x is a unit if and only if $\delta(x) = \delta(1)$.

Gaussian Integers: The subset $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ of the complex numbers is called the set of Gaussian integers. As $\mathbb{C}$ is a field and hence an integral domain, $\mathbb{Z}[i]$ is also an integral domain.

The units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

The ring $\mathbb{Z}[i]$ is a ED, hence a PID and hence a UFD.