1. Rings, subrings and fields

- **Ring R**: set with binary operations addition and subtraction, where $(R, +)$ is an abelian group and:
  - **Identity**: exists $1 \in R$ such that $\forall x \in R, 1 \cdot x = x \cdot 1 = x$
  - **Associativity**: for every $x, y, z \in R, x(yz) = (xy)z$
  - **Distributivity**: for every $x, y, z \in R, x(y + z) = xy + xz$ and $(y + z)x = yx + zx$
- **Set of remainders modulo n (residue classes)**: $\mathbb{Z} / n = \left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\}$
- $\mathbb{Z} / n$ is a ring: $\overline{a} + \overline{b} = \overline{a+b}, \overline{a} - \overline{b} = \overline{a-b}, \overline{a} \cdot \overline{b} = \overline{a \cdot b}$
- **Subring S** of ring R: a set $S \subseteq R$ that contains 0 and 1 and is closed under addition, multiplication and negation:
  - $0 \in S, 1 \in S$
  - $\forall a, b \in S, a + b \in S$
  - $\forall a, b \in S, ab \in S$
  - $\forall a \in S, -a \in S$
- **Field F** is a ring with:
  - F is commutative
  - $0 \neq 1 \in F$ (F has at least two elements)
  - $\forall 0 \neq a \in R, \exists b \in R, ab = 1$. b is the **inverse** of a
- a is a **zero divisor** if $ab = 0$ for some $b \neq 0$

2. Integral domains

- **Integral domain R**: ring which is commutative, has at least two elements ($0 \neq 1$), and has no zero divisors apart from 0
- Any subring of a field is an integral domain
- If R is an integral domain, then $R[x] = \{a_0 + a_1 x + ... + a_n x^n : a_i \in R\}$ is also an integral domain.
- a is a **unit** if $ab = ba = 1$ for some $b \in R$. $b = a^{-1}$ is the **inverse** of a
- Inverses are unique
- $R^{\times}$, set of all units in R, is a group under multiplication of R
- For field F, $F^{\times} = F - \{0\}$
- $a \in \mathbb{Z} / n$ is a unit iff $\gcd(a, n) = 1$
- $\mathbb{Z} / p$ is a field iff p is prime
- $\mathbb{Z} / n$ is an integral domain iff n is prime (iff $\mathbb{Z} / n$ is a field)

3. Polynomials over a field

- **Degree** of $f(x) = a_0 + a_1 x + ... + a_n x^n$:

$$\deg(f) = \begin{cases} \max\{i : a_i \neq 0\} & \text{if } f \neq 0 \\ -\infty & \text{if } f = 0 \end{cases}$$

- $\deg(fg) = \deg(f) + \deg(g)$
- $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
- If $\deg(f) \neq \deg(g)$ then $\deg(f + g) = \max\{\deg(f), \deg(g)\}$

- Let $f(x), g(x) \in F[x]$, $g(x) \neq 0$, then $\exists q(x), r(x) \in F[x]$ with $\deg(r) < \deg(g)$ such that $f(x) = q(x)g(x) + r(x)$

4. Divisibility and greatest common divisor in a ring

- a **divides** b, $a \mid b$, if $\exists r \in R$ such that $b = ra$
- d is a **greatest common divisor** of a and b, $\gcd(a, b)$, if:
  - $d \mid a$ and $d \mid b$ and
  - If $e \mid a$ and $e \mid b$ then $e \mid d$
- $\gcd(0, 0) = 0$
- **Euclidean algorithm example**: find gcd of $f(x) = x^2 + 7x + 6$ and $g(x) = x^2 - 5x - 6$ in $\mathbb{Q}[x]$:

$$\begin{aligned} f(x) &= g(x) + 12(x+1) \\ g(x) &= \frac{1}{12}x \cdot 12(x+1) - 6(x+1) \\ 12(x+1) &= -2 \cdot -6(x+1) + 0 \end{aligned}$$

  Remainder is now zero so stop. A gcd is given by the last non-zero remainder, $-6(x+1)$. We can write $-6(x+1)$ as a combination of $f(x)$ and $g(x)$:

$$\begin{aligned} -6(x+1) &= g(x) - \frac{1}{12}x \cdot 12(x+1) \\ &= g(x) - \frac{1}{12}x \cdot (f(x) - g(x)) \\ &= \left(1 + \frac{1}{12}x\right)g(x) - \frac{1}{12}xf(x) \end{aligned}$$

- Let R be integral domain, $a, b \in R$ and $d = \gcd(a, b)$. Then $\forall u \in R^\times$, ud is also a $\gcd(a, b)$. Also, for d and d' gcds of a and b, $\exists u \in R^\times$ such that $d = ud'$ (so gcd is unique up to units).
- Polynomial is **monic** if leading coefficient is 1
- There always exists a unique monic gcd of two polynomials in $F[x]$
- Let $R = \mathbb{Z}$ or $F[x]$, $a, b \in R$. Then
  - A $\gcd(a, b)$ always exists
  - $a \neq 0$ or $b \neq 0$ then a $\gcd(a, b)$ can be computed by Euclidean algorithm
  - If d is a $\gcd(a, b)$ then $\exists x, y \in R$ such that $ax + by = d$

5. Factorisations in rings

- $r \in R$ **irreducible** if:
  - $r \notin R^\times$ and
  - If $r = ab$ then $a \in R^\times$ or $b \in R^\times$
- $a \in F$ is **root** of $f(x) \in F[x]$ if $f(a) = 0$
- Let $f(x) \in F[x]$.
  - If $\deg(f) = 1$, f is irreducible.
  - If $\deg(f) = 2$ or 3 then f is irreducible iff it has no roots in F.

- If $\deg(f) = 4$ then f is irreducible iff it has no roots in F and it is not the product of two quadratic polynomials.
- Let $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[x]$, $\deg(f) \geq 1$. If $f(p / q) = 0$, $\gcd(p, q) = 1$, then $p \mid a_0$ and $q \mid a_n$.
- **Gauss's lemma**: let $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[x]$, $\deg(f) \geq 1$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ iff it is irreducible in $\mathbb{Q}[x]$ and $\gcd(a_0, a_1, ..., a_n) = 1$.
- If monic polynomial in $\mathbb{Z}[x]$ factors in $\mathbb{Q}[x]$ then it factors into integer monic polynomials.
- Let R be commutative, $x \in R$ be irreducible and $u \in R^\times$. Then ux is also irreducible.
- **Eisenstein's criterion**: let $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[x]$, p be prime with $p \mid a_0$, $p \mid a_1, ..., p \mid a_{n-1}$, $p \nmid a_n$, $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$
- Let $f(x) \in F[x]$, then f can be uniquely factorised into a product of irreducible elements, up to order of factors and multiplication by units.
- Let R be commutative. $x \in R$ is **prime** if:
  - $x \neq 0$ and $x \notin R^\times$ and
  - If $x \mid ab$ then $x \mid a$ or $x \mid b$
- If $R = \mathbb{Z}$ or $F[x]$ then $a \in R$ is prime iff it is irreducible.
- Let R be an integral domain and $x \in R$ prime. Then x is irreducible.
- Integral domain R is **unique factorisation domain (UFD)** if every non-zero non-unit element in R can be written as a unique product of irreducible elements, up to order of factors and multiplication by units.

6. Ring homomorphisms

- For R, S rings, $f : R \to S$ is **homomorphism** if:
  - $f(1) = 1$ and
  - $f(a + b) = f(a) + f(b)$ and
  - $f(ab) = f(a)f(b)$
- Let $f : R \to S$ homomorphism, then
  - $f(0) = 0$ and
  - $f(-a) = -f(a)$
- **Kernel**:

$$\ker(f) := \{a \in R : f(a) = 0\}$$

- **Image**:

$$\mathrm{Im}(f) := \{f(a) : a \in R\}$$

- **Isomorphism**: bijective homomorphism.
- R and S **isomorphic**, $R \cong S$ if there exists isomorphism between them.
- Homomorphism f injective iff $\ker(f) = \{0\}$.
- **Direct product** of R and S, $R \times S$:
  - $(r, s) + (r', s') = (r + r', s + s')$.
  - $(r, s)(r', s') = (rr', ss')$.
  - Identity is $(1, 1)$.

- For $p_1(r, s) = r$ and $p_2(r, s) = s$, $\ker(p_1) = \{(0, s) : s \in S\}$ and $\ker(p_2) = \{(r, 0) : r \in R\}$. These are both rings, with $\ker(p_1) \cong S$ (via $(0, s) \to s$) and $\ker(p_2) \cong R$ (via $(r, 0) \to r$). ($\ker(p_1)$ and $\ker(p_2)$ are not subrings of $R \times S$ though). So

$$\ker(p_1) \times \ker(p_2) \cong R \times S$$

7. Ideals and quotient rings

- $I \subseteq R$ is an **ideal** if I closed under addition and if $x \in I$, $r \in R$ then $rx \in I$ and $xr \in I$.
- **Left ideal**: I closed under addition and if $x \in I$, $r \in R$ then $rx \in I$.
- **Right ideal**: I closed under addition and if $x \in I$, $r \in R$ then $xr \in I$.
- If $x \in I$, then $(-1)x = x(-1) = -x \in I$ so I closed under negation.
- For $f : R \to S$ homomorphism, $\ker(f)$ is ideal of R.
- For R commutative ring and $a \in R$, **principal ideal generated by a** is

$$(a) := \{ra : r \in R\}$$

- For R commutative and $a_1, ...a_n \in R$,

$$(a_1, ..., a_n) := \{r_1 a_1 + \dots + r_n a_n : r_1, ..., r_n \in R\}$$

  is an ideal. $(a_1, ..., a_n)$ is **generated** by $a_1, ..., a_n$. $a_i \in (a_1, ..., a_n)$ for all i.
- If ideal I contains unit u, then $u^{-1}u = 1 \in I$ so $\forall r \in R, r \cdot 1 = r \in I$. So $R \subseteq I$ so $R = I$.
- For field F, any ideal is either $\{0\}$ or F.
- Let $I_1 = (a_1, ..., a_m)$, $I_2 = (b_1, ..., b_n)$ then $I_1 = I_2$ iff $a_1, ..., a_m \in I_2$ and $b_1, ..., b_n \in I_1$.
- $a, b \in R$ **equivalent modulo I** if $a - b \in I$. Write $\overline{a} = \overline{b}$ or $a \equiv b \pmod{I}$.
- Let $a(x) \in \mathbb{Q}[x]$, then $p(x) = q(x)a(x) + r(x)$ with $\deg(r) < \deg(a)$. $p(x) - r(x) = q(x)a(x) \in (a(x))$ so $\overline{p(x)} = \overline{r(x)}$. $r(x)$ is **representative** of the class $\overline{p(x)}$.
- Let $I \subseteq R$ ideal. **Coset** of I generated by $x \in I$ is

$$\overline{x} := x + I = \{x + r : r \in I\} \subseteq R$$

  x is a **representative** of $x + I$.
- For $x, y \in R$,

$$x + I = y + I \Longleftrightarrow x + I \cap y + I \neq \emptyset \Longleftrightarrow x - y \in I$$

- If x is a representative of $x + I$, so is $x + r$ for every $r \in I$.
- **Quotient** of R by I ("$R \bmod I$"): set of all cosets of R by I:

$$R / I := \{\overline{x} : x \in R\} = \{x + I : x \in R\}$$

  with
  - $(x + I) + (y + I) = (x + y) + I$.
  - $(x + I)(y + I) = xy + I$.
- R / I is a ring, with zero element $0 + I = I$ and identity $1 + I \in R / I$.
- **Quotient map (canonical map/homomorphism)**: $R \to R / I, r \to \overline{r} = r + I$.
- Kernel of quotient map is I and image is R / I. Hence every ideal is a kernel.

- **First isomorphism theorem (FIT)**: Let $\varphi : R \to S$ be homomorphism. Then

$$\overline{\varphi} : R \,/\, \ker(\varphi) \to \operatorname{Im}(\varphi), \overline{\varphi}(\overline{x}) = \varphi(x)$$

  is an isomorphism: $R \,/\, \ker(\varphi) \cong \operatorname{Im}(\varphi)$.

8. Prime and maximal ideals

- Ideal $I \subseteq R$ **prime ideal** if $I \neq R$ and $ab \in I \Longrightarrow a \in I$ or $b \in I$.
- $I \subseteq R$ **maximal** if only ideals containing I are I and R (so no ideals strictly between I and R).
- $x \in R$ is prime iff (x) is prime ideal.
- To contain is to divide:

$$a \in (x) \Longleftrightarrow (a) \subseteq (x) \Longleftrightarrow x \mid a$$

- For R commutative and I ideal:
  - I prime iff $R \,/\, I$ integral domain.
  - I maximal iff $R \,/\, I$ field.
- (I, x) is ideal generated by I and x:

$$(I, x) : \{rx + x' : r \in R, x' \in I\}$$

- If I is maximal ideal, then it is prime.

9. Principal ideal domains

- **Principal ideal domain (PID)**: integral domain where every ideal is principal.
- $\mathbb{Z}$, $F[x]$, $\mathbb{Z}[i]$ and $\mathbb{Z}\left[\sqrt{\pm 2}\right]$ are PIDs.
- Every PID is a UFD.
- Let R be PID and $a, b \in R$. Then $d = \gcd(a, b)$ exists and $(d) = (a, b)$.

10. Fields as quotients

- Let R be PID, $a \in R$ irreducible. Then (a) is maximal.
- Let $f(x) \in F[x]$ irreducible. Then $F[x] \,/\, (f(x))$ is field and $F[x] \,/\, (f(x))$ is a vector space over F with basis $\left\{\overline{1}, \overline{x}, ..., \overline{x}^{n-1}\right\}$ where $n = \deg(f)$. So every element in $F[x] \,/\, f(x)$ can be uniquely written as $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$, $a_i \in F$.
- Let p prime and $n \in \mathbb{N}$, then there exists irreducible $f(x) \in (\mathbb{Z} \,/\, p)[x]$ with $\deg(f) = n$ and $(\mathbb{Z} \,/\, p)[x] \,/\, (f(x))$ is a field with p^n elements. Any two such fields are isomorphic so unique (up to isomorphism) field with p^n elements is written $\mathbb{F}_{p^n}$.

11. The Chinese remainder theorem

- $a, b \in R$ **coprime** if no irreducible element divides a and b.
- Let R be PID, $a, b \in R$ coprime. Then $(a, b) = (1) = R$ so $ax + by = 1$ for some $x, y \in R$. So any $\gcd(a, b)$ is a unit.
- **Chinese remainder theorem (CRT)**: Let R be PID, $a_1, ..., a_k$ pairwise coprime. Then

$$\varphi : R \,/\, (a_1 \cdots a_k) \to R \,/\, (a_1) \times \cdots \times R \,/\, (a_k)$$
$$\varphi(r + (a_1 \cdots a_k)) = (r + (a_1), ..., r + (a_k))$$

is an isomorphism.

12. Basics of groups

- **Group** $(G, \circ)$: set G with binary operation $\circ : G \times G \to G$ satisfying:
  - **Closure**: $g \circ h \in G, h \circ g \in G$.
  - **Associativity**: $a \circ (b \circ c) = (a \circ b) \circ c$.
  - **Identity**: $g \circ e = g$ and $e \circ g = g$ for some $e \in G$.
  - **Inverse**: $g \circ h = h \circ g = e$ for some $h = g^{-1} \in G$.
- Group **abelian** if $\circ$ commutative: $g \circ h = h \circ g$.
- $H \subseteq G$ is **subgroup** of $(G, \circ)$, $H < G$ if H is group under same operation.
- Subgroup H **proper** if $H \neq \{e\}$ and $H \neq G$.
- **Subgroup criterion**: $H < G$ iff:
  - H non-empty.
  - $h_1, h_2 \in H \Longrightarrow h_1 \circ h_2 \in H$.
  - $h \in H \Longrightarrow h^{-1} \in H$.
- **Order** of group G is number of elements in it, $|G|$.
- **Lagrange's theorem**: Let G finite, $H < G$, then

$$\#H \mid \#G$$

- Let $H < G$, $g \in G$. **Left coset** of g with respect to H in G:

$$g \circ H := \{g \circ h : h \in H\}$$

- All left cosets with respect to H have same cardinality as cardinality of H.
- **Right coset** of $g \in G$ with respect to $H < G$ in G:

$$H \circ g := \{h \circ g : h \in H\}$$

- $H < G$ **normal**, $H \triangleleft G$, if $\forall g \in G, gH = Hg$.
- H is normal iff $\forall g \in G$,

$$\forall h \in H, ghg^{-1} \in H \Longleftrightarrow gHg^{-1} \subset H$$

  where $gHg^{-1} = \left\{ghg^{-1} : h \in H\right\}$.
- Every subgroup of abelian group is normal.
- **Subgroup of G generated by g**:

$$\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$$

- **Subgroup of G generated by $S \subseteq G$**:

$$\langle S \rangle := \{\text{all finite products of elements in } S \text{ and their inverses}\}$$

  so if G abelian (doesn't hold for non-abelian), for $S = \left\{g_1, ..., g_n\right\}$,

$$\langle S \rangle = \left\{g_1^{a_1} \cdots g_n^{a_n} : a_i \in \mathbb{Z}\right\}$$

- If G not abelian,

$$\langle g, h \rangle = \left\{g^{a_1} h^{b_1} \cdots g^{a_m} h^{a_m}\right\}$$

- **Order** of $g \in G$, $\mathrm{ord}_G(g)$ is smallest $r > 0$ such that $g^r = e$. If r doesn't exist, order is ∞.

- Order of $\overline{m} \in \mathbb{Z} / n$ is $n / \gcd(m, n)$.

13. Specific families of groups

- Quaternion group:

$$Q_8 = \{\pm 1 \pm i, \pm j, \pm k\}, \quad i^2 = j^2 = k^2 = -1, ij = k = -ji$$

- **Cyclic group**: can be generated by single element.
- **Example of cyclic group**:

$$C_n = \left\{ e^{\frac{2\pi i}{n} k} : 0 \leq k < n \right\}$$

- Cyclic groups are abelian.
- If $|G|$ is prime, G is cyclic and is generated by any $e \neq g \in G$.
- **Permutation** of $X \neq \emptyset$: bijection $X \to X$.
- $S_X := \{\text{bijection } X \to X\}$.
- **Notation**: $S_n := S_{\{1,\dots,n\}}$.
- $(S_X, \circ)$ is group where $\circ$ is composition of permutations.
- $(S_n, \circ)$ is **symmetric group of degree n** (or **symmetric group on n letters**).
- **Notation**: write $\sigma \in S_n$ as

$$\begin{bmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{bmatrix}$$

- $|S_n| = n!$.
- **Cycle of length k (or k-cycle)**: permutation σ in S_n, with

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \quad \sigma(i_k) = i_1$$

  and leaves all other elements fixed. Write as $(i_1\ i_2\ \dots\ i_k)$ or

$$\begin{bmatrix} i_1 & i_2 & \dots & i_k \\ i_2 & i_3 & \dots & i_1 \end{bmatrix}$$

- 2-cycles are **transpositions** (or **inversions**).
- k-cycle has order k.
- There are k ways of writing k cycle.
- Cycles are **disjoint** if they don't have any common elements.
- Disjoint cycles commute.
- Every permutation is product of disjoint cycles, unique up to swapping cycles and k ways of writing a k-cycle.
- k-cycle can be written as product of transpositions:

$$(i_1\ i_2\ \dots\ i_k) = (i_1\ i_2)(i_2\ i_3) \cdots (i_{k-1}\ i_k)$$

- When composing cycles, **work right to left**.
- $g, g' \in G$ **conjugate** in G to each other if for some $h \in G$, $hgh^{-1} = g'$.
- Any conjugate of transposition in S_n is transposition.
- Every $\sigma \in S_n$ can be factored into product of transpositions.

- **Parity** of number of transpositions needed in any factorisation of σ is the same. So remainder of this number modulo 2 is well-defined.
- Element made of disjoint cycles of lengths $k_1, ..., k_m$ has order $\operatorname{lcm}(k_1, ..., k_m)$.
- **Sign of permutation $\boldsymbol{\sigma}$**:

$$\operatorname{sgn}(\sigma) := (-1)^t = \begin{cases} 1 & \text{if } t \text{ is even} \\ -1 & \text{if } t \text{ is odd} \end{cases}$$

  where t is number of transpositions needed in factorisation of σ. If t even, σ is **even**, else σ is **odd**.
- **Alternating group**, A_n: subgroup of even permutations of S_n.
- $|A_n| = \frac{n!}{2}$.
- A_n normal in S_n.
- A_n generated by 3-cycles.
- **Isometry**: map from plane to itself which preserves distances between points.
- For $n \geq 3$, there are $2n$ isometries of the plane which preserve regular n-gon.
- Group of isometries of regular n-gon form group, the **dihedral group**, D_n.
- D_n **alternative definition**: group with two generators r (rotation) and s (reflection), with $srs^{-1} = r^{-1}$, $r^n = e$ and $s^2 = e$. So $D_n = \langle r, s \rangle$.
- Every element in D_n can be written $r^j s^k$, $0 \leq j < n$, $0 \leq k \leq 1$.
- $|D_n| = 2n$.
- Rotations of plane which preserve regular n-gon form cyclic subgroup of D_n, which is normal in D_n.

14. Relating, identifying and distinguishing groups

- **Group homomorphism**: map $\varphi : G \to G'$ between groups, with

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$$

- **Group isomorphism**: bijective group homomorphism.
- G and G' **isomorphic**, $G \cong G'$ if exists isomorphism between them.
- **Kernel** of group homomorphism:

$$\ker(\varphi) := \{g \in G : \varphi(g) = e\}$$

- **Image** of group homomorphism:

$$\operatorname{im}(\varphi) := \{\varphi(g) : g \in G\}$$

- $\ker(\varphi)$ is normal subgroup of G.
- $\operatorname{im}(\varphi)$ is subgroup of G'.
- Let N normal subgroup of G. **Quotient group (factor group)** of G with respect to N, is $G / N := \{gN : g \in G\}$, with group multiplication

$$(g_1 N)(g_2 N) = (g_1 g_2) N$$

  and inverse

$$(gN)^{-1} = (g^{-1}) N$$

- **First isomorphism theorem for groups (FIT)**: let $\varphi : G \to G'$ homomorphism, then
$$G \mathbin{/} \ker(\varphi) \cong \operatorname{im}(\varphi)$$
- Let p prime, then every group of order p is isomorphic to $(\mathbb{Z} \mathbin{/} p, +)$.
- Each cyclic group of order n isomorphic to $(\mathbb{Z} \mathbin{/} n, +)$.
- Each infinite cyclic group isomorphic to $(\mathbb{Z}, +)$.
- For groups G, H, $G \times H$ also a group, with $e = (e_G, e_H)$, $(g, h) \circ (g', h') = (g \circ_G g', h \circ_H h')$, inverse $(g, h)^{-1} = \left(g^{-1}, h^{-1}\right)$.
- $\mathbb{Z} \mathbin{/} 2 \times \mathbb{Z} \mathbin{/} 3 \cong \mathbb{Z} \mathbin{/} 6$.
- $\mathbb{Z} \mathbin{/} (mn) \cong \mathbb{Z} \mathbin{/} m \times \mathbb{Z} \mathbin{/} n \Longleftrightarrow \gcd(m, n) = 1$.
- Group isomorphism preserves:
  - Order of group.
  - Set of orders of elements (with multiplicity - i.e. count repeated occurences of an order).
  - Size of its centre.
  - Property of being abelian/non-abelian.
  - Property of having proper (normal) subgroups and their sizes.
- **Notation**: for $E_1, E_2 \subseteq G$,
$$E_1 \circ E_2 := \{e_1 \circ e_2 : e_1 \in E_1, e_2 \in E_2\}$$
- Let H, K subgroups of G with:
  - $H \circ K = G$,
  - $H \cap K = \{e\}$,
  - $\forall h \in H, k \in K, hk = kh$.

  Then $G \cong H \times K$.
- Group of symmetries of unit cube in $\mathbb{R}^3$ isomorphic to S_4.
- **Cayley's theorem**: Every group $(G, \cdot)$ is isomorphic to a subgroup of $(S_G, \circ)$ where S_G is set of bijections of G by the isomorphism $\psi(g) = L_g$, where $L_g(h) = gh$.

15. Group actions

- **Action of group G on non-empty set X**: homomorphism
$$\varphi : G \to S_X$$
  G acts on X.
- Let $\varphi : G \to S_X$ group action, $x \in X$. **Orbit** of x inside X is
$$G(x) := \mathcal{O}(x) := \{\varphi(g)(x) : g \in G\}$$
- Let $\varphi : G \to S_X$ group action, $x \in X$. **Stabiliser** of x in G is
$$G_x := \operatorname{Stab}_G(x) := \{g \in G : \varphi(g)(x) = x\}$$
- For every $x \in X$, $\operatorname{Stab}_G(x)$ is subgroup of G.
- **Notation**: can write $g(x)$ instead of $\varphi(g(x))$.
- Let $\varphi : G \to S_X$ group action. Then all orbits $\mathcal{O}(x)$ partition X so:
  - Every orbit non-empty subset of X.
  - Union of all orbits is X.
  - Two orbits either disjoint or equal.

- Action of group on itself:
  - By left translation: $g(h) = gh$.
  - By conjugation: $g(h) = ghg^{-1}$.
- **Conjugacy class** of $g \in G$ is set of all elements conjugate to g:

$$\text{ccl}_G(g) := \left\{hgh^{-1} : h \in G\right\}$$

- Conjugacy class of g is orbit of conjugation action of g.
- Conjugacy classes of G all of size 1 iff G abelian.
- **Orbit-stabiliser theorem**: Let G act on X. Then $\forall x \in X$, exists bijection

$$\beta : \mathcal{O}(x) \to \{\text{left cosets of } \text{Stab}_G(x) \text{ in } G\}$$
$$\beta(g(x)) = g\text{Stab}_G(x)$$

- **Consequence of Orbit-Stabiliser theorem**: if finite G acts on finite X, then $\forall x \in X$,

$$|\mathcal{O}(x)| \cdot |\text{Stab}_G(x)| = |G|$$

- So size of each conjugacy class in G divides $|G|$.
- If $x \in \mathcal{O}(y)$, then $\text{Stab}_G(x)$ and $\text{Stab}_G(y)$ conjugate to each other:

$$\exists h \in G, \quad \text{Stab}_G(x) = h\text{Stab}_G(y)h^{-1}$$

  (here $h(y) = x$).

16. Cauchy's theorem and classification of groups of order $2p$

- **Cauchy's theorem**: let G finite group, p prime, $p \mid |G|$. Then exists subgroup of G of order p.
- Let p odd prime, then any group of order $2p$ is either cyclic or dihedral.

17. Classification of groups of order p^2

- **Centre** of group G:

$$Z(G) := \{g \in G : \forall h \in G, gh = hg\}$$

- $Z(G)$ is normal subgroup of G.
- $Z(G)$ is union of all conjugacy classes of size 1. So every $z \in Z(G)$ has $|\text{ccl}_G(z)| = 1$.
- $Z(G) = G$ iff G abelian.
- If G acts on itself via conjugation then for every $h \in G$, $Z(G) \subset \text{Stab}_G(h)$.
- Let p prime, $|G| = p^r$, $r \geq 0$. Then $Z(G)$ non-trivial ($Z(G) \neq \{e\}$).
- If $|G| = p^2$, p prime, then G abelian.
- Let p prime, $|G| = p^2$. Then $G \cong \mathbb{Z} / p^2$ or $G \cong \mathbb{Z} / p \times \mathbb{Z} / p$.
- **Sylow's theorem**: let G group, $|G| = p^r m$, $\gcd(p, m) = 1$. Then G has subgroup of order p^r (and subgroup of order p^i for all $1 \leq i \leq r$).

18. Classification of finitely generated abelian groups

- G **finitely generated** if exists set $\left\{g_1, ..., g_r\right\}$ such that $G = \langle g_1, ..., g_r\rangle$.
- Any finitely generated abelian group can be written as

$$G \cong \mathbb{Z}^n / K$$

for some $n \geq 0$, K is subgroup of $\mathbb{Z}^n$, $K = \left\{\underline{a} \in \mathbb{Z}^n : a_1 g_1 + \cdots + a_n g_n = 0\right\}$. $\underline{a} \in K$ is **relation** and K is **relation subgroup** of G.

- G is **free abelian group of rank n** if no non-trivial solutions in K, i.e. $a_1 g_1 + \cdots + a_r g_r = 0 \Longrightarrow a_1 = \cdots = a_r = 0$. Here, $K = \{\underline{0}\}$.
- Every subgroup of $\mathbb{Z}^n$ is free abelian group generated by $r \leq n$ elements, so rank $\leq n$.
- **Fundamental theorem of finitely generated abelian groups**: let G be finitely generated abelian group. Then

$$G \cong \mathbb{Z} / d_1 \times \cdots \times \mathbb{Z} / d_k \times \mathbb{Z}^r$$

where $r \geq 0$, $k \geq 0$, $d_j \geq 1$. If $d_1 \mid d_2 \mid \cdots \mid d_k$ and $d_1 > 1$, then this form is unique.
- r is **rank** of G, $d_1, \ldots, d_k$ are **torsion invariants (torsion coefficients)**. Torsion coefficients are given with repetitions (multiplicities).
- To classify all groups of order n, use that $d_1 \cdots d_k = n$ and $1 < d_1 \mid d_2 \mid \cdots \mid d_k$.
- Let $e \neq x \in S_n$ be written as product of disjoint cycles:

$$x = \left(a_1\ a_2\ \ldots\ a_{k_1}\right)\left(b_1\ b_2\ \ldots\ b_{k_2}\right) \cdots \left(t_1\ t_2\ \ldots\ t_{k_r}\right)$$

where $r \geq 1$, $2 \leq k_1 \leq k_2 \leq \cdots \leq k_r$, $n \geq k_1 + \cdots + k_r$. Then x has **cycle shape** $[k_1, k_2, \ldots, k_r]$.
- Let $x = (i_1\ i_2\ \ldots\ i_k) \in S_n$, $g \in S_n$. Then action of g on x by conjugation is

$$g x g^{-1} = (g(i_1)\ g(i_2)\ \ldots\ g(i_k))$$

- Let $x \in S_n$, then $\operatorname{ccl}_{S_n}(x)$ consists of all permutations with same cycle shape as x.
- Conjugacy classes of S_n have cycle shapes given by non-decreasing partitions of n, without 1 (except for cycle shape [1]).
- Let $x = (a_1\ a_2\ \ldots\ a_m) \in S_n$, then

$$\gamma(n; m) := \left|\operatorname{ccl}_{S_n}(x)\right| = \frac{n(n-1) \cdots (n-m+1)}{m}$$

- Let $x \in S_n$ have cycle shape $[m_1, \ldots, m_r]$, $m_1 < m_2 < \cdots < m_r$. Then

$$\gamma(n; m_1, \ldots, m_r) := \left|\operatorname{ccl}_{S_n}(x)\right| = \prod_{k=1}^{r} \gamma\left(n - \sum_{i=1}^{k-1} m_i; m_k\right)$$

- Let $x \in S_n$ has cycle shape $[m_1, \ldots, m_1, m_2, \ldots, m_2, \ldots, m_r, \ldots, m_r]$, $m_1 < m_2 < \cdots < m_r$, m_i repeated s_i times, then number of elements of that cycle shape is

$$\left|\operatorname{ccl}_{S_n}(x)\right| = \frac{\gamma(n; m_1, \ldots, m_1, m_2, \ldots, m_2, \ldots, m_r, \ldots, m_r)}{s_1! s_2! \cdots s_r!}$$

- Let H subgroup of G. Then H normal in G iff H is union of conjugacy classes of G.
- So if H normal then sum of sizes of its conjugacy classes divides $|G|$. But converse doesn't imply H is subgroup.
- To find all normal subgroups H of S_n, use that size of H is sum of sizes of conjugacy classes of S_n. Use formula above to work out all possible sizes of conjugacy classes, and fact that H must contain identity so must include 1 in its sum (size of conjugacy class of 1

is 1). Then use Lagrange's theorem to restrict the possible sums of the sizes. Then check that each set formed by the union is a group.