0.1. Functions

0.1.1. *Definition.* A function $f: X \to Y$ is called

- *injective* if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$ (equivalently, if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$).
- *surjective* if for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$.
- *bijective* if it is both injective and surjective.

If f is bijective, we denote its inverse function by f^{-1}.

1.1. Symmetries of graphs

1.1.1. *Definition.* (similar to [L, §9]). A *graph* is a finite set of vertices joined by edges. We will assume that there is at most one edge joining two given vertices and no edge joins a vertex to itself. The *valency* of a vertex is the number of edges emerging from it.

1.1.3. *Definition.* A *symmetry* of a graph is a permutation of the vertices that preserves the edges. More precisely, let V denote the set of vertices of a graph. Then a symmetry is a bijection $f: V \to V$ such that $f(v_1)$ and $f(v_2)$ are joined by an edge if and only if v_1 and v_2 are joined by an edge.

1.2. Groups and Examples

1.2.1. *Definition.* [J, §4.2] Let S be any nonempty set. An operation $*$ on S is a rule which, for every ordered pair (a, b) of elements of S, determines a unique element $a * b$ of S. Equivalently, if we recall that

$$S \times S := \{(a, b) \mid a, b \in S\},$$

then an operation is a function $S \times S \to S$.

1.2.3. *Definition.* **(Definition of a Group)** [J, §4.3] We say that a nonempty set G is *group under* $*$ if

G1. (Closure) $*$ is an operation, so $g * h \in G$ for all $g, h \in G$.
G2. (Associativity) $g * (h * k) = (g * h) * k$ for all $g, h, k \in G$.
G3. (Identity) There exists an *identity element* $e \in G$ such $e * g = g * e = g$ for all $g \in G$.
G4. (Inverses) Every element $g \in G$ has an *inverse* g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Further, if G is a group, the number of elements in G is written $|G|$, and is called the *order* of G.

1.2.4. *Theorem.* The symmetries of a graph forms a group (under composition).

1.3. Symmetries of regular n-gons (=dihedral groups)

1.3.2. *The dihedral group.* Consider now a regular n-gon (where $n \geq 3$). Its symmetry group is called the *dihedral group* D_n. It has precisely $2n$ elements,

1.4. Symmetries of finite sets (=the symmetric group)

1.4.1. *Symmetric groups.* A symmetry of a set X of n objects is a *permutation* (i.e. a bijection $X \to X$). The set of all symmetries of X is denoted S_n. It has precisely $n!$ elements.

1.5. (Rotational) Symmetries of regular solids

Recall [L, p77–78] that there are five platonic solids "fire, earth, air, ether and water", convex bodies whose faces are all the same regular n-gon, where every vertex is identical. They are:

	Faces	Edges	Vertices	Faces per vertex
tetrahedron	4 triangles	6	4	3
hexahedron	6 squares	12	8	3
octahedron	8 triangles	12	6	4
dodecahedron	12 pentagons	30	20	3
icosahedron	20 triangles	30	12	5

1.6. Symmetries of vector spaces

1.6.1. *Definition.* The set of *invertible* $n \times n$ matrices with coefficients in $\mathbb{R}$ is denoted $\mathrm{GL}(n, \mathbb{R})$. Similarly, if p is a prime, then the set of invertible $n \times n$ matrices with coefficients in $\mathbb{Z}_p$ is denoted $\mathrm{GL}(n, \mathbb{Z}_p)$.

1.6.2. *Theorem.* $\mathrm{GL}(n, \mathbb{R})$ is a group under matrix multiplication.

Similarly, when p is a prime, $\mathrm{GL}(n, \mathbb{Z}_p)$ is a group under matrix multiplication.

2.1. First basic properties

2.1.1. *Lemma.* Let G be a group. If $g, h \in G$, then

1. There is one and only one element $k \in G$ such that $k * g = h$.
2. There is one and only one element $k \in G$ such that $g * k = h$.

2.1.3. *Corollaries.* (see also [J, §4.5])

1. In a group you can always cancel: if $g * s = g * t$ then $s = t$. Similarly, if $s * g = t * g$ then $s = t$.
2. Inverses are unique: given $g \in G$ then there is one and only one element $h \in G$ such that $g * h = e$. In particular, $e^{-1} = e$ and $(g^{-1})^{-1} = g$.
3. A group has only one identity: if $g * h = h$ (even just for one particular h) then $g = e$.

2.2. **Commutativity**

2.2.1. *Definition.* Suppose that G is a group and $g, h \in G$. If $g * h = h * g$ then we say that g and h *commute*. If $g * h = h * g$ for all $g, h \in G$, then we say G is an *abelian* group.

2.3. **Products**

2.3.1. *Theorem.* Let G, H be groups. The product $G \times H = \{(g, h) \mid g \in G, h \in H\}$ has the natural structure of a group as follows:

- The group operation is $(g, h) * (g', h') := (g *_G g', h *_H h')$ (where we write $*_G$ for the group operation in G, etc).
- The identity e in $G \times H$ is $e := (e_G, e_H)$ (where we write e_G for the identity in G, etc).
- The inverse of (g, h) is (g^{-1}, h^{-1}) (the inverse of g is taken in G, and the inverse of h is taken in H).

2.3.3. *Note.* If G, H are both finite then

$$|G \times H| = |G|\,|H|\,.$$

2.4. **Subgroups**

2.4.1. *Definition.* [J, §5] Let G be a group. We say that a nonempty subset H of G is a *subgroup* of G if H itself is a group (under the operation from G). We write

$H \leq G$ if H is a subgroup of G. If also $H \neq G$, we write $H < G$ and say that H is a proper subgroup.

2.4.2. *Lemma.* Suppose that $H \leq G$. Then

1. $e_H = e_G$
2. If $h \in H$, the inverse of h in H equals the inverse of h in G.

2.4.3. *Theorem.* (Test for a subgroup) $H \subseteq G$ is a subgroup of G if and only if

S1. H is not empty.

S2. If $h, k \in H$ then $h * k \in H$

S3. If $h \in H$ then $h^{-1} \in H$.

2.5. **Order of elements**

2.5.1. *Definition.* (Order of a group) A *finite group* G is one with only a finite number of elements. The *order* of a finite group, written $|G|$, is the number of elements in G.

2.5.2. *Definition.* (Order of an element) [J, §6.3] Let G be a group and $g \in G$. Then the *order* $o(g)$ of g is the *least* natural number n such that

$$\underbrace{g * \dots * g}_{n} = e.$$

If no such n exists, we say that g has infinite order.

2.5.4. *Theorem.* In a finite group, every element has finite order.

2.5.5. *Corollary.* Let g be an element of a finite group G. Then there exists $k \in \mathbb{N}$ such that $g^k = g^{-1}$.

2.6. **Cyclic subgroups**

2.6.1. *Definition.* If G is a group, $g \in G$ and $k \in \mathbb{Z}$, define

$$\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\} = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}.$$

If G is finite, then $\langle g \rangle$ (being a subset of G) is finite, and we can think of $\langle g \rangle$ as

$$\langle g \rangle = \{e, g, \dots, g^{o(g)-1}\}$$

2.6.2. *Lemma.* If G is a group and $g \in G$, then $\langle g \rangle$ is a subgroup of G.

2.6.3. *Definition.* A subgroup $H \leq G$ is *cyclic* if $H = \langle h \rangle$ for some $h \in H$. In this case, we say that H is the *cyclic subgroup generated by h*. If $G = \langle g \rangle$ for some $g \in G$, then we say that the group G is *cyclic*, and that g is a *generator*.

2.6.6. *Theorem.* Let G be a cyclic group and let H be a subgroup of G. Then H is cyclic.

2.6.7. *Theorem.* Let $m, n \in \mathbb{N}$, let $G = \langle g \rangle$ be a cyclic group of order m and $H = \langle h \rangle$ be a cyclic group of order n. Then

$$G \times H \text{ is cyclic} \iff m \text{ and } n \text{ are coprime (i.e. } \gcd(m, n) = 1).$$

3.1. Recap on Equivalence relations

3.1.1. *Definition.* [L,§18] Let X be a set, and R a subset of $X \times X$ (thus R consists of some ordered pairs (s,t) with $s,t \in X$). If $(s,t) \in R$ we write $s \sim t$ and say "s is related to t". We call $\sim$ a *relation* on X.

A relation $\sim$ is called an *equivalence relation* on X if

R. (Reflexive) $x \sim x$ for all $x \in X$
S. (Symmetric) $x \sim y$ implies that $y \sim x$ for all $x, y \in X$
T. (Transitive) $x \sim y$ and $y \sim z$ implies that $x \sim z$ for all $x, y, z \in X$.

3.2. Proof of Lagrange: cosets

3.2.1. *Notation.* Let A, B be subsets of a group G and let $g \in G$. Then

$$AB := \{ab \mid a \in A, b \in B\}, \quad gA := \{ga \mid a \in A\},$$

and similarly for other obvious variants.

3.2.2. *Definition.* [J, §10.1] Let $H \leq G$ and let $g \in G$. Then a *left coset* of H in G is a subset of G of the form gH, for some $g \in G$.

3.2.4. *Definition.* We denote G/H to be the set of left cosets of H in G.

3.2.5. *Lemma.* Suppose that $H \leq G$, then $|gH| = |H|$ for all $g \in G$.

3.2.6. *Theorem.* Let $H \leq G$.

1. For all $h \in H$, $hH = H$. In particular $eH = H$.
2. For $g_1, g_2 \in G$, the following are equivalent
   (a) $g_1 H = g_2 H$.
   (b) there exists $h \in H$ such that $g_2 = g_1 h$.
   (c) $g_2 \in g_1 H$.
3. For a fixed $g \in G$, the number of $g_1 \in G$ such that $gH = g_1 H$ is equal to $|H|$.
4. For $g_1, g_2 \in G$, define $g_1 \sim g_2$ if and only if $g_1 H = g_2 H$. Then $\sim$ defines an equivalence relation on G.

3.2.7. *Corollaries.* [J, §10] Suppose that G is a finite group.

1. **(Lagrange's theorem)** If $H \leq G$, then $|H|$ divides $|G|$.
2. Let $g \in G$. Then $o(g)$ divides $|G|$.
3. For all $g \in G$, we have that $g^{|G|} = e$.

3.2.8. *Corollary.* $|G/H| = \frac{|G|}{|H|}$.

3.2.9. *Definition.* The *index* of $H \leq G$ is defined to be the number of *distinct* left cosets of H in G, which by above is $|G/H| = \frac{|G|}{|H|}$.

3.2.10. *Definition.* The *right cosets* of H in G are subsets of the form Hg.

3.3. **First applications of Lagrange**

3.3.1. *Theorem.* Suppose that G is a group with $|G| = p$, where p is prime. Then G is a cyclic group.

3.3.2. *Corollary.* Suppose that G is a group with $|G| < 6$. Then G is abelian.

3.3.3. *Theorem.* (Fermat's Little Theorem) If p is a prime and $a \in \mathbb{Z}$, then

$$a^p \equiv a \bmod p.$$

3.3.4. *Theorem.* If p is a prime, then

1. In $\mathbb{Z}_p^*$ only 1 and $p-1$ are their own inverses.
2. (Wilson's Theorem) $(p-1)! \equiv -1 \bmod p$.

4.1. **Homomorphisms and Isomorphisms**

4.1.1. *Definition.* Let G, H be groups. A map $\phi : G \to H$ is called a *group homomorphism* if

$$\phi(xy) = \phi(x)\phi(y) \quad \text{for all } x, y \in G.$$

4.1.2. *Definition.* A group homomorphism $\phi : G \to H$ that is also a bijection is called an *isomorphism* of groups. In this case we say that G and H are *isomorphic* and we write $G \cong H$. An isomorphism $G \to G$ is called an *automorphism* of G.

4.1.5. *Lemma.* Let $\phi\colon G \to H$ be a group homomorphism. Then

1. $\phi(e) = e$ and further $\phi(g^{-1}) = (\phi(g))^{-1}$ for all $g \in G$.
2. If ϕ is injective, the order of $g \in G$ equals the order of $\phi(g) \in H$.

4.1.6. *Definition.* Let $\phi\colon G \to H$ be a group homomorphism.

1. The *image* of ϕ is defined to be

$$\operatorname{im}\phi := \{h \in H \mid h = \phi(g) \text{ for some } g \in G\}$$

2. We define the *kernel* of ϕ to be

$$\operatorname{Ker}\phi := \{g \in G \mid \phi(g) = e_H\}.$$

4.1.7. *Proposition.* Let $\phi\colon G \to H$ be a group homomorphism. Then

1. $\phi : G \to H$ is injective if and only if $\ker\phi = \{e_G\}$.
2. If $\phi : G \to H$ is injective, then ϕ gives an isomorphism $G \cong \operatorname{im}\phi$.

4.2. Products and Isomorphisms

4.2.1. *Definition.* (reminder) If S and T are subsets of G, then we define

$$ST := \{st \mid s \in S,\ t \in T\}.$$

4.2.2. *Theorem.* [J, §14.3] Let $H, K \leq G$ be subgroups with $H \cap K = \{e\}$.

1. The map $\phi : H \times K \to HK$ given by $\phi : (h, k) \mapsto hk$ is bijective.
2. If further every element of H commutes with every element of K when multiplied in G (i.e. $hk = kh$ for all $h \in H, k \in K$), then HK is a subgroup of G, and furthermore it is isomorphic to $H \times K$, via ϕ.

4.2.4. *Corollary.* Let $H, K \leq G$ be finite subgroups of a group G with $H \cap K = \{e\}$. Then $|HK| = |H| \times |K|$.

5.1. Definition of a group action

5.1.1. *Definition.* Let G be a group, and let X be a nonempty set. Then a (left) action of G on X is a map

$$G \times X \to X,$$

written $(g, x) \mapsto g \cdot x$, such that

$$g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x \quad \text{and} \quad e \cdot x = x$$

for all $g_1, g_2 \in G$ and all $x \in X$.

5.2. Faithful actions

5.2.1. *Proposition.* Suppose G acts on X. Define

$$N := \{g \in G \mid g \cdot x = x \text{ for all } x \in X\}.$$

Then N is a subgroup of G.

5.2.2. *Definition.* Suppose that G acts on X, then the subgroup N defined above in §5.2.1 is called the *kernel* of the action. Note in [J] it is denoted Ker $\cdot$, but this notation is quite hard to read. If $N = \{e\}$ then we say that the action is *faithful.*

Thus an action is faithful if $g \cdot x = x$ for all $x \in X$ implies that $g = e$. In words "the only member of G that fixes everything in X is the identity".

5.3. Every group lives inside a symmetric group

If X is a set, we denote

$$\text{bij}(X) := \{\text{bijections } X \to X\}.$$

5.3.1. *Lemma.* [J, 7.4] If G acts on a set X, then for all $g \in G$ the map

$$f_g \colon X \to X$$

defined $x \mapsto g \cdot x$ is a bijection.

5.3.2. *Theorem.* [J, 7.4, 9.3] Let G be a group, and let X be a set. Then

1. An action of G on X is equivalent to a group homomorphism $\phi : G \to \mathrm{bij}(X)$.
2. The action is faithful if and only if ϕ is injective.
3. If the action is faithful, then ϕ gives an isomorphism of G with $\mathrm{im}\,\phi \leq \mathrm{bij}(X)$.

5.3.3. *Corollary.* **(Cayley's Theorem)** Every finite group is isomorphic to a subgroup of a symmetric group.

5.4. Orbits and Stabilizers

5.4.1. *Definition.* Let G act on X, and let $x \in X$. The *stabilizer* of x is defined to be

$$\mathrm{Stab}_G(x) := \{g \in G \,|\, g \cdot x = x\}.$$

5.4.2. *Lemma.* For all $x \in X$, the stabilizer $\mathrm{Stab}_G(x)$ is a subgroup of G.

5.4.3. *Definition.* Let G act on X, and let $x \in X$. The *orbit* of x under G is

$$\mathrm{Orb}_G(x) = \{g \cdot x \,|\, g \in G\}.$$

5.4.5. *Theorem.* [J, 8.4] Let G act on X. Then

$$x \sim y \iff y = g \cdot x \text{ for some } g \in G$$

defines an equivalence relation on X. The equivalence classes are the orbits of G. Thus when G acts on X, we obtain a partition of X into orbits.

5.4.7. *Definition.* An action of G on X is *transitive* if for all $x, y \in X$ there exists $g \in G$ such that $y = g \cdot x$. Equivalently, X is a single orbit under G.

5.4.9. *Notation.* [J, top p87] Suppose G acts on X and $x, y \in X$. If y and x are in the same orbit,

$$\mathrm{send}_x(y) := \{g \in G \mid g \cdot x = y\}$$

is a non-empty subset of G.

5.4.11. *Theorem.* [J, p117] Let G act on X, let $x \in X$, and set $H := \mathrm{Stab}_G(x)$ Then the map

$$\mathrm{send}_x \colon \mathrm{Orb}_G(x) \to G/H \quad \text{which sends} \quad y \mapsto \mathrm{send}_x(y)$$

is a bijective map of *sets.*

5.4.12. *Corollary.* **(The orbit-stabilizer theorem)** Suppose G is a finite group acting on a set X, and let $x \in X$. Then $|\mathrm{Orb}_G(x)| \times |\mathrm{Stab}_G(x)| = |G|$, or in words

5.4.14. *Theorem.* **(Cauchy's Theorem)** Let G be a group, p be a prime. If p divides $|G|$, then G contains an element of order p.

5.5. **Pólya counting**

5.5.1. *Theorem.* [J, 11.3] Let G be a finite group acting on a finite set X. For $g \in G$ define

$$\mathrm{Fix}(g) := \{x \in X \mid g \cdot x = x\}$$

(so that $|\mathrm{Fix}(g)|$ is the number of elements of X that g fixes). Then

$$\text{the number of orbits in } X = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| .$$

6.1. **Symmetric and Alternating Groups**

6.1.1. *Definition.* Let $n \in \mathbb{N}$, let $1 \leq r \leq n$ and let $\{a_1, a_2, \dots, a_r\}$ be r distinct numbers between 1 and n. The *cycle* $(a_1\, a_2\, \dots\, a_r)$ denotes the element of S_n that sends a_1 to a_2, a_2 to a_3, ..., a_{r-1} to a_r, a_r to a_1, and leaves the remaining $n - r$ numbers fixed. We say that the *length* of the cycle $(a_1\, a_2\, \dots\, a_r)$ is r.

6.1.2. *Definition.* Two cycles $(a_1\, a_2\, \dots\, a_r)$ and $(b_1\, b_2\, \dots\, b_s)$ are *disjoint* if

$$\{a_1, a_2, \dots, a_r\} \cap \{b_1, b_2, \dots, b_s\} = \emptyset.$$

6.1.4. *Theorem.* Every permutation can be written as a product of disjoint cycles.

6.1.6. *Definition.* Given $\sigma \in S_n$, write σ as a product of disjoint cycles, as in §6.1.4. In this product, for each $t = 1, \dots, n$ let m_t denote the number of cycles of length t. Then we say that σ has *cycle type*

$$\underbrace{1, \dots, 1}_{m_1}, \underbrace{2, \dots, 2}_{m_2}, \dots, \underbrace{n, \dots, n}_{m_n},$$

As notation for cycle type, we usually abbreviate this to $1^{m_1}, 2^{m_2}, \dots, n^{m_n}$.

6.1.8. *Theorem.* The number of elements of S_n of cycle type $1^{m_1}, 2^{m_2}, \dots, n^{m_n}$ is

$$\frac{n!}{m_1! \dots m_n! 1^{m_1} 2^{m_2} \dots n^{m_n}}.$$

6.1.10. *Definition.* Let $n \in \mathbb{N}$ and set

$$P = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Let $X = \{P, -P\}$. Then S_n acts on X by

$$\sigma \cdot P = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$$

If $\sigma \in S_n$ has the property that $\sigma \cdot P = P$, we say that σ is *even*. If $\sigma \cdot P = -P$, we say that σ is *odd*.

6.1.11. *Theorem.* Let A_n denote the set of all even permutations in S_n. Then A_n is a subgroup of S_n, with $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$. We call A_n the *alternating group.*

7.1. **Conjugate elements**

7.1.1. *Definition/ Lemma.* Let $h \in G$ and $g \in G := X$. Then

$$h \cdot g := hgh^{-1}$$

defines an action of a group G on itself, called the *conjugation action*. The orbits are called the *conjugacy classes* of G. Under this action, the stabilizer of an element $g \in G$ is precisely

$$C(g) := \{h \in G \mid gh = hg\}.$$

which we define to be the *centralizer* of g in G.

7.1.3. *Definition.*

1. We say that g, g' are *conjugate* if there exists $h \in G$ such that $g' = hgh^{-1}$. That is, two elements are conjugate if they lie in the same conjugacy class.
2. [J, 13.5] We define the *centre* of a group G to be

$$C(G) := \{g \in G \mid gh = hg \text{ for all } h \in G\}.$$

   If $g \in C(G)$, we say that g is *central.*

7.1.5. *Corollaries.*

1. For all $g \in G$, the centralizer $C(g)$ is a subgroup of G.
2. The centre $C(G)$ is a subgroup of G.
3. If G is finite and $g \in G$, then

$$(\text{the number of conjugates of } g \text{ in } G) \times |C(g)| = |G|.$$

4. $\{e\}$ is always a conjugacy class of G
5. $\{g\}$ is a conjugacy class if and only if $g \in C(G)$. Hence $C(G)$ is the union of all the one-element conjugacy classes.

7.1.6. *Theorem.* Suppose that G is a finite group with conjugacy classes $C_1, \dots, C_n$. We adopt the convention that $C_1 = \{e\}$. Let the conjugacy classes have sizes $c_1, \dots, c_n$ (so that $c_1 = 1$).

1. If $g \in C_k$, then $c_k = \frac{|G|}{|C(g)|}$. In particular, c_k divides the order of the group.
2. We have

$$|G| = c_1 + c_2 + \dots + c_n,$$

   and further each of the c_j divides $|G|$. This is called the *class equation* of G.

7.2. Conjugacy in S_n is determined by cycle type

7.2.1. *Lemma.* Let $\sigma \in S_n$, and write σ as a product of disjoint cycles, say $\sigma = (a_1 \dots a_r)(b_1 \dots b_s) \dots$. Then for all $\tau \in S_n$,

$$\tau\sigma\tau^{-1} = (\tau(a_1) \dots \tau(a_r))(\tau(b_1) \dots \tau(b_s)) \dots$$

which is a product of disjoint cycles.

7.2.2. *Theorem.* Two permutations in S_n are conjugate if and only if they have the same cycle type (up to ordering).

7.3. Normal subgroups

7.3.1. *Definition.* A subgroup N of G is *normal* if

$$gng^{-1} \in N \quad \text{for all } g \in G \text{ and all } n \in N.$$

We write $N \trianglelefteq G$ if N is a normal subgroup of G.

7.3.3. *Theorem.* Let N be a subgroup in G, then N is a normal subgroup if and only if N is a union of conjugacy classes.

7.3.4. *Corollary.* If G is a group, then $C(G) \trianglelefteq G$.

7.3.5. *Lemma.*

1. Let $\phi : G \to H$ be a group homomorphism. Then $\ker \phi \trianglelefteq G$.
2. (Recall §5.2.1) Suppose that G acts on X, then the kernel of the action

$$N := \{g \in G \mid g \cdot x = x \text{ for all } x \in X\}$$

is a normal subgroup of G.

7.3.6. *Lemma.* Let $N \leq G$. Then the following are equivalent:

1. N is normal in G.
2. $gNg^{-1} = N$ for all $g \in G$.
3. $gN = Ng$ for all $g \in G$.

7.3.7. *Theorem.* Let $H \leq G$ with $\frac{|G|}{|H|} = 2$. Then H is normal in G.

7.3.9. *Definition.* We say that a group G is *simple* if the only normal subgroups of G are $\{e\}$ and G.

7.4. Factor groups

7.4.2. *Theorem.* G/H is a group under $g_1H * g_2H := g_1g_2H \iff H$ is a normal subgroup of G.