ALGEBRA II

EDWARD O'CALLAGHAN

Contents

1. Prelude

TODO: Fix notation here...

We define the non-zero complex numbers form a multiplicative group, written:

$$\mathbb{C}^{\times} \doteq \mathbb{C} - \{0\}.$$

2. Introduction

In this course we build up the rudiments of some important notions of algebraic structures. That is, a algebraic structure of an arbitrary set, or carrier set, coupled with various finitary operations defined on it. ..

3. Groups

Definition 3.1 (Binary operation)**.** A **binary operation** on a set $\mathcal{X}$ is a map $\circ : \mathcal{X} \times \mathcal{X} \to \mathcal{X}'$. **N.B.** that the binary operation need not be closed.

Definition 3.2 (Magma)**.** A **magma** is a set $\mathcal{M}$ equipped with a binary operation $\circ$ that is closed under the operation on $\mathcal{M}$. We denote the magma as the tuple pair $(\mathcal{M}, \circ)$.

Definition 3.3 (Semi-group)**.** A **semi-group** is a set $\mathcal{G}$ equipped with binary operation that is *associative*. Hence, a semi-group is a magma where the operation is *associative*; That is, given any $x, y, z \in \mathcal{G}$ then $x \circ (y \circ z) = (x \circ y) \circ z \in \mathcal{G}$. We denote the semi-group as the tuple pair $(\mathcal{G}, \circ)$, not to be confused with a magma from context.

Definition 3.4 (Monoid)**.** A **semi-group with idenitity** or, **monoid** for short, is a semi-group $(\mathcal{G}, \circ)$ with a unique identity element $e \in \mathcal{G}$ such that $x \circ e = x = e \circ x \, \forall x \in \mathcal{G}$

Proof: unquieness of idenitity. Assume some other identity $e^{'}$ exists in $\mathcal{G}$ then, $e^{'} = e^{'} \circ e = e \circ e^{'} = e$. $\square$

Example 3.5. Given $\mathcal{G} = \mathbb{N}$ with the binary law of composition $\circ$ to be defined as arithmetic addition $+$. Then, $(\mathbb{N}, +)$ forms a semi-group with identity 0. Verify the axioms.

Definition 3.6 (Group)**.** A **group** is a monoid where every element has an inverse. An abelian group is a group that is commutative.

Example 3.7. Given $\mathcal{G} = \mathbb{Z}$ with the binary law of composition $\circ$ to be defined as arithmetic addition $+$. Then, $(\mathbb{Z}, +)$ forms a semi-group with identity 0. Verify the axioms.

Question 3.8. *Why does the set of naturals $\mathbb{N}$ not form a group under multiplication, however does form a monoid?*

Definition 3.9 (Group order)**.** If a group $\mathcal{G}$ has n finitely many elements the *order*, denoted $|\mathcal{G}| = n$, is the number of elements of $\mathcal{G}$.

Definition 3.10 (Group element order)**.** For a element g in some group $\mathcal{G}$ the order of g is defined to be the least positive integer k such that $g^k = e$, where e denotes the group identity, with respect to the groups law of composition. In symbols, $o(g) = k$. If no such k exists then g is said to have infinite order.

Remark. A non-trivial element, $g \neq e$, of finite order, $o(g) = k < \infty$, is called a *torsion element* and for when $k = 2$ it is called an *involution*.

Theorem 3.11. *Every finite group of even order has a non-trivial involution. That is, for some group $\mathcal{G}$ where $|\mathcal{G}| = 2n < \infty$ we have that, there exists some non-trivial element $g \neq e$ in $\mathcal{G}$ such that $g^2 = e$.*

Example 3.12 (Matrix Groups)**.** Linear maps of vector spaces form groups that have characteristic properties. For some vector space $\mathcal{V}$ over some field $\mathbb{F}$ we may define the following groups taking matrix multiplication as the binary law of composition.

i.) The *General Linear* group defined by,
$$GL(\mathbb{F}) \doteq \{M \in \mathcal{M} : det(M) \neq 0\}.$$

ii.) The *Special Linear* group defined by,
$$SL(\mathbb{F}) \doteq \{M \in GL(\mathbb{F}) : \det(M) = 1\}.$$

iii.) The *Orthogonal* group defined by,
$$O(\mathbb{R}) \doteq \{M \in GL(\mathbb{R}) : M^T M = I\}.$$

iv.) The *Special Orthogonal* group defined by,
$$SO(\mathbb{R}) \doteq \{M \in O(\mathbb{R}) : \det(M) = 1\}.$$

v.) The *Unitary* group defined by,
$$U(\mathbb{C}) \doteq \{M \in GL(\mathbb{C}) : M^* M = I\}.$$

vi.) The *Special Unitary* group defined by,
$$SU(\mathbb{C}) \doteq \{M \in U(\mathbb{C}) : \det(M) = 1\}.$$

Example 3.13 (Lorentz Group)**.** The Lorentz group is defined as,
$$\mathcal{L}(\mathbb{R}) \doteq \{M \in \mathcal{M}_2(\mathbb{R}) : M^T C M = C\}$$
where C describes the Lorentz inner product with respect to the standard basis, i.e.
$$C = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Definition 3.14 (Automorphism Group)**.** Suppose $\mathcal{S} = (S, *)$ is some algebraic structure and $\mathbb{S}$ is the set of automorphism of $\mathcal{S}$. Then we may define the structure $(\mathbb{S}, \circ)$, where $\circ$ is defined as functional composition, as the *group of automorphisms* of $\mathcal{S}$, denoted $Aut(\mathcal{S})$ or $\mathscr{A}(\mathcal{S})$. That is,

$$\mathscr{A}(\mathcal{S}) \doteq (\mathbb{S}, \circ) \text{ where } \mathbb{S} \doteq \{\phi : \mathcal{S} \to \mathcal{S}, \text{ where } \phi \text{ is a bijection.}\}$$

For some algebraic structure $\mathcal{S}$ on set S.

3.1. **Cyclic Groups.**

3.1.1. *Generating Sets.*

Definition 3.15 (Generating Set)**.** For some $S \subseteq \mathcal{G}$ define $S^{-1} = \{s^{-1} : s \in S\}$ and let $\langle S \rangle$ denote the set of all elements of $\mathcal{G}$ that can be written as finite products of elements of $S \cup S^{-1}$. That is,

$$\langle S \rangle \doteq \{g \in \mathcal{G} : g = s_0 \dots s_n \text{ where } s_i \in S \cup S^{-1}\}.$$

Lemma 3.16. *The generating set $\langle S \rangle$ is a subgroup of $\mathcal{G}$, called the* subgroup generated by *S.*

Definition 3.17 (Finitely Generated)**.** Let $\mathcal{G}$ be a group. Then $\mathcal{G}$ is said to be *finitely generated* if there is a finite set $S \subseteq \mathcal{G}$ such that $\mathcal{G} = \langle S \rangle$.

Example 3.18. Consider the group $\mathcal{G} = \mathbb{Z}_5^\times$ and notice that $\mathcal{G} = \langle 2 \rangle$. Since,

$$\begin{aligned}
2^1 &= 2, \\
2^2 &= 4, \\
2^3 &= 8 \equiv 3 \pmod 5, \\
2^4 &= 16 \equiv 1 \pmod 5
\end{aligned}$$

and so the element 2 is a generator of the multiplicative group $\mathbb{Z}_5 - \{0\}$.

3.1.2. *Cyclic Groups.*

Definition 3.19 (Cyclic group)**.** A group $\mathcal{G}$ is *cyclic* if $\mathcal{G} = \mathrm{Gp}(g)$ for some $g \in \mathcal{G}$. Such a element is called a *generator* of the group.

3.2. **Permutations.** Take a finite set X with $|X| = n$, then the transformations of X are called **permutations** of the elements of X. In particular, the group of permutations of $X = \{1, 2, \cdots, n\}$ is a **symmetric group**, denoted S_n, with **order** $|S_n| = n!$. Thus, by taking any subgroup of S_n we have a **permutation group**. Also note that, for finite sets, *permutation* and *bijective maps* refer to the same operation, namely rearrangement of elements of X. Another way is to consider, a group $\mathcal{G}$ and set X. Then a group action is defined as a group homomorphism φ from $\mathcal{G}$ to the symmetric group of X. That is, the action $\varphi : \mathcal{G} \to S_n(X)$, assigns a permutation of X to each element of the group $\mathcal{G}$ in the following way:

- From the identity element $e \in \mathcal{G}$ to the identity transformation id_X of X, that is, $\varphi : e \to id_X$;
- A product of group homomorphisms $\varphi \circ \psi \in \mathcal{G}$ is then the composite of permutations given by φ and ψ in X.

Given that each element of $\mathcal{G}$ is represented as a permutation. Then a group action can also be consider as a permutation representation.

A permutation $\sigma \in S_n$ can be written,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \text{ where } a_1 = \sigma(1), a_2 = \sigma(2), \cdots .$$

The identity permutation $id_n \in S_n$ is simply,

$$id_n = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

.

Since $|S_n| = n!$ then the total number of ways n elements maybe permuted is $n!$.

Take any two permutations $\sigma, \pi \in S_n$ then composition is well defined as **functional composition** as follows.

Given,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \text{ } and \text{ } \pi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$$

then,

$$\begin{aligned} \pi \circ \sigma &= \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(a_1) & \pi(a_2) & \cdots & \pi(a_n) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} \end{aligned}$$

.

A inverse of any permutation $\sigma \in S_n$ is given by,

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}^{-1} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

3.3. **Permutation parity.** Consider the algebraic structure:

$$\triangle_n(x_1, \ldots, x_n) = \prod_{i<j}(x_i - x_j)$$

TODO..

3.4. **Symmetric Group.** TODO FIX sections??

Definition 3.20 (Dihedral group)**.** The *dihedral group* $\mathcal{D}_n$ is defined as the symmetries of a regular n-gon. The order $|\mathcal{D}_n| = 2n$ as there are n rotations and n reflections.

3.5. **Group actions.** For any mathematical object (e.g. sets, groups, vector spaces) X an isomorphism of X is a symmetry of X. The set of all isomorphisms of X, or symmetries of X, form a group called the symmetry group of X, denoted $Sym(X)$. More formally;

Definition 3.21 (Group action)**.** An *action* of a group $\mathcal{G}$ on a mathematical object X is a mapping $\mathcal{G} \times X \to X$, defined by $(g, x) \mapsto g.x$ satisfying:

- $e.x = x \, \forall x \in X$ and
- $(gh).x = g.(h.x) \, \forall g, h \in \mathcal{G}, x \in X$.

That is, we have the (*left*) $\mathcal{G}$-action on X and denote this by $\mathcal{G} \curvearrowright X$.

Notice that we may study properties of the symmetries of some mathematical object X without reference to the structure of X in particular.

3.6. **Subgroups.**

Definition 3.22 (Subgroup)**.** A group $\mathcal{H}$ is a **subgroup** of a group $\mathcal{G}$ if the restriction of the binary operation $\circ : \mathcal{H} \times \mathcal{H} \to \mathcal{H}$ is a group operation on $\mathcal{H}$. In particular, A non-empty subset $\mathcal{H}$ of a group $\mathcal{G}$ is a subgroup of $\mathcal{G}$ if and only if $h_1 \circ h_2 \in \mathcal{H}$ whenever $h_1, h_2 \in \mathcal{H}$, and $h^{-1} \in \mathcal{H}$ whenever $h \in \mathcal{H}$. We denote the subgroup by $\mathcal{H} \leq \mathcal{G}$.

Theorem 3.23 (Smallest subgroup)**.** *If $\mathcal{A}$ is a subset of a group $\mathcal{G}$, there is a* smallest *subgroup $Gp(\mathcal{A})$ of $\mathcal{G}$ which contains $\mathcal{A}$, the subgroup* generated *by $\mathcal{A}$.*

Example 3.24. Suppose $\mathcal{A} = \{g\}$ then $\mathrm{Gp}(\mathcal{A}) = \mathrm{Gp}(g)$ and so $\mathrm{Gp}(g) = \{g^n : n \in \mathbb{Z}\}$, where $g^0 = e$, g^n is the product of n copies of g where $n > 0$, and g^n is the product of $|n|$ copies of g^{-1} when $n < 0$.

Definition 3.25 (Normal subgroup)**.** A subgroup $\mathcal{H}$ of a group $\mathcal{G}$ is a **normal**, or *self-conjugate*, if $ghg^{-1} = h$ for all $g \in \mathcal{G}$ and for all $h \in \mathcal{H}$. We denote the normal $\mathcal{H} \trianglelefteq \mathcal{G}$.

Definition 3.26 (Simple group)**.** A group $\mathcal{G}$ is **simple** if it has no normal subgroups other than the trivial normal subgroups $\{e\}$ and $\mathcal{G}$.

3.6.1. *Sylow's Theorems.* The Norwegian mathematician *Ludwig Sylow* established some important results while investigating subgroups of prime order.

Definition 3.27 (p-subgroup)**.** TODO.

Definition 3.28 (Sylow p-subgroup)**.** TODO.

Theorem 3.29 (First Sylow Theorem)**.** *Let p be prime and $\mathcal{G}$ be a group such that $|\mathcal{G}| = kp^n$ where $p \not| k$. Then $\mathcal{G}$ has* at least *one Sylow p-subgroup.*

Theorem 3.30 (Second Sylow Theorem)**.** *Let P be a Sylow p-subgroup of some finite group $\mathcal{G}$. Let Q be any p-subgroup of $\mathcal{G}$. Then Q is contained in a conjugate of P.*

Theorem 3.31 (Third Sylow Theorem)**.** *All the Sylow p-subgroups of a finite group are conjugate.*

Theorem 3.32 (Fourth Sylow Theorem)**.** *The number of Sylow p-subgroups of a finite group is congruent to $1(\mod p)$.*

Theorem 3.33 (Fifth Sylow Theorem)**.** *The number of Sylow p-subgroups of a finite group is a divisor of their common subgroup index.*

We now look at a representation theorem for groups known as Cayley's Theorem. This theorem informs us that; In order to study finite groups it is only necessary to study subgroups of the symmetric group. In particular,

Theorem 3.34 (Cayley's Theorem)**.** *Let S_n denote the symmetric group on n letters. Every finite group is isomorphic to a subgroup of S_n for some $n \in \mathbb{Z}$.*

Proof. Let $\mathcal{H} = \{e\}$. By applying permutation of Cosets to $\mathcal{H}$ so that $\mathbb{S} = \mathcal{G}$ and $\ker(\theta) = \{e\}$. The result follows by the First Isomorphism Theorem. □

Definition 3.35 (Characteristic Subgroup)**.** Let $\mathcal{G}$ be a group and $\mathcal{H}$ be a subgroup $\mathcal{H} \leq \mathcal{G}$ such that for every $\phi \in Aut(\mathcal{G})$ we have $\phi(\mathcal{H}) = \mathcal{H}$, where $Aut(\mathcal{G})$ denotes the group of automorphisms of $\mathcal{G}$. Then $\mathcal{H}$ is *characteristic in* $\mathcal{G}$, or *a characteristic subgroup of* $\mathcal{G}$.

Theorem 3.36 (Characteristic Subgroup Transivity)**.** *Suppose $\mathcal{G}$ is a group and let $\mathcal{H}$ be a characteristic subgroup of $\mathcal{G}$ and $\mathcal{K}$ a characteristic subgroup of $\mathcal{H}$. Then $\mathcal{K}$ is a characteristic subgroup of $\mathcal{G}$.*

Proof. Let $\phi : \mathcal{G} \to \mathcal{G}$ be a group automorphism. Since $\mathcal{H}$ is a characteristic subgroup of $\mathcal{G}$, by definition, we have that

$$\phi(\mathcal{H}) = \mathcal{H}.$$

That is, the restriction of ϕ to $\mathcal{H}$, written $\phi|_{\mathcal{H}}$, is a automorphism of $\mathcal{H}$. Now, since $\mathcal{K}$ is a characteristic subgroup of $\mathcal{H}$, we have that

$$\phi|_{\mathcal{H}}(\mathcal{K}) = \mathcal{K}$$
$$\Rightarrow \phi(\mathcal{K}) = \mathcal{K}$$

and so $\mathcal{K}$ is a characteristic subgroup pf $\mathcal{G}$. □

3.7. **Group Homomorphisms.** Homomorphisms are structure preserving mappings. In group homomorphisms we preserve the group structure, defined by the binary law of composition. In particular,

Definition 3.37 (Group Homomorphism)**.** Let $(\mathcal{G}, \circ)$ and $(\mathcal{H}, \dagger)$ be two groups. Then a mapping $\varphi : \mathcal{G} \to \mathcal{H}$ is called a *group homomorphism* if

$$\varphi(g_1 \circ g_2) = \varphi(g_1) \dagger \varphi(g_2) : g_1, g_2 \in \mathcal{G}.$$

It follows that, for some $g \in \mathcal{G}$ we have,

$$\begin{aligned}\varphi(e_g) &= \varphi(g \circ g^{-1}) \\ &= \varphi(g) \dagger \varphi(g^{-1}) \\ &= \varphi(g) \dagger (\varphi(g))^{-1} \\ &= e_h \in \mathcal{H}.\end{aligned}$$

That is the identity e has been preserved.

In this way, it does not matter if we compose in $\mathcal{G}$ and map to $\mathcal{H}$ or take two elements in $\mathcal{G}$ then compose the mapped elements in $\mathcal{H}$, since the group structure has been preserved.

How much information about the elements inside the structure is, however, another quality to consider. Hence we fix some terminology here.

- A homomorphism that is injective is called monomorphic.
- A homomorphism that is surjective is called epimorphic.
- A homomorphism that is bijective is called isomorphic.

Thus we have the following definitions by considering a group homomorphism $\varphi : \mathcal{G} \to \mathcal{H}$.

Definition 3.38 (Monomorphic)**.** φ is **monomorphic** if for $\varphi(x) = \varphi(y) \implies x = y \, \forall x, y \in \mathcal{G}$.

Definition 3.39 (Epimorphic)**.** φ is **epimorphic** if $\forall h \in \mathcal{H} \exists g \in \mathcal{G}$ so that $\varphi(g) = h$.

Definition 3.40 (Isomorphic)**.** φ is **isomorphic** if φ is **both** mono- and epic- morphic.

Some special cases are sometimes of particular interest and we shall outline them now.

Definition 3.41 (Endomorphic)**.** A monomorphism $\mathcal{G} \to \mathcal{G}$ for a group $\mathcal{G}$ is called an *endomorphism* of $\mathcal{G}$.

Definition 3.42 (Automorphic)**.** A isomorphism $\mathcal{G} \to \mathcal{G}$ for a group $\mathcal{G}$ is called an *automorphism* of $\mathcal{G}$.

Remark. The set $Aut(\mathcal{G})$ of automorphisms of $\mathcal{G}$ forms a group, when composition of mappings is taken as the group law of composition.

Example 3.43 (Trivial Homomorphism)**.** The trivial group homomorphism $id_{\mathcal{G}} : \mathcal{G} \to \mathcal{G}$, given by the mapping $g \mapsto g$ for every $g \in \mathcal{G}$, is in fact a group automorphism.

Example 3.44. Consider $\psi : GL_n(\mathbb{R}) \to \mathbb{R}^{\times}$ defined by the mapping $A \mapsto \det(A)$ and recall that $\det(AB) = \det(A)\det(B)$. That is, the determinant is a group homomorphism.

Example 3.45. Consider $\psi : \mathcal{G} \to S_n/A_n$ where $\mathcal{G} = \{-1, 1\}$, defined by $1 \mapsto A_n$ and $-1 \mapsto (1\,2)A_n$, and observe that ϕ is a group homomorphism.

Problem 3.46. *Consider the map $\phi : \mathbb{R} \to SL_2(\mathbb{R})$ defined by,*

$$x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Show that $\phi(x + y) = \phi(x) \cdot \phi(y)$. Also, prove that ϕ is injective.

Example 3.47. Consider the map $\exp : \mathbb{R}^{+} \to \mathbb{R}^{\times}$ from the additive to the multiplicative group, defined by $x \mapsto e^x$, is a group homomorphism. Since, $\exp(x + y) = \exp(x) \cdot \exp(y)$.

Example 3.48. Consider the linear transformation $T : \mathcal{V} \to \mathcal{W}$. By definition of linearity, $T(\vec{v}_1 + \vec{v}_2) = T(\vec{v}_1) + T(\vec{v}_2)$, the mapping T is a group homomorphism from the additive group of vector space $\mathcal{V}$ to the additive group of vector space $\mathcal{W}$.

Problem 3.49. *Suppose $N \trianglelefteq \mathcal{G}$ and $\pi : \mathcal{G} \to \mathcal{G}/N$, given by the mapping $g \mapsto gN$ for every $g \in \mathcal{G}$. Show that π is a group homomorphism and then show that it is surjective.*

Problem 3.50. *Suppose $\phi : \mathbb{C}^{\times} \to \mathbb{R}^{\times}$ given by the mapping $z \mapsto |z|$. Show that ϕ is a group homomorphism. Is ϕ bijective?*

Proposition 3.51. *Let $\varphi : \mathcal{G} \to \mathcal{H}$ be a group homomorphism.*

i.) $\varphi(1_{\mathcal{G}}) = 1_{\mathcal{H}}$,
ii.) $\varphi(g^{-1}) = \varphi(g)^{-1}$ *for all* $g \in \mathcal{G}$,
iii.) If $\mathcal{G}' \leq \mathcal{G}$ *then* $\varphi(\mathcal{G}') \leq \mathcal{H}$ *when the restriction* $\mathcal{H} = \varphi|_{\mathcal{G}'}(\mathcal{G})$ *holds,*
iv.) If φ *is an isomorphism, then so is its inverse* $\varphi^{-1} : \mathcal{H} \to \mathcal{G}$,
v.) If $\psi : \mathcal{G} \to \mathcal{H}$ *and* $\varphi : \mathcal{H} \to \mathcal{K}$ *are group homomorphisms then so is* $\varphi \circ \psi$.

Proof. For *i.*) we see that,

$$\begin{aligned} 1_{\mathcal{H}} \cdot \varphi(1_{\mathcal{G}}) &= \varphi(1_{\mathcal{G}}) && \text{(and that)} \\ \varphi(1_{\mathcal{G}}) &= \varphi(1_{\mathcal{G}} \circ 1_{\mathcal{G}}) \\ &= \varphi(1_{\mathcal{G}}) \cdot \varphi(1_{\mathcal{G}}) \end{aligned}$$

so we have that,

$$\begin{aligned} 1_{\mathcal{H}} \cdot \varphi(1_{\mathcal{G}}) &= \varphi(1_{\mathcal{G}}) \\ \Rightarrow 1_{\mathcal{H}} \cdot \varphi(1_{\mathcal{G}}) \cdot \varphi(1_{\mathcal{G}})^{-1} &= \varphi(1_{\mathcal{G}}) \cdot \varphi(1_{\mathcal{G}})^{-1} \\ \Rightarrow 1_{\mathcal{H}} &= \varphi(1_{\mathcal{G}}). \end{aligned}$$

□

Proof. For *ii.*) we see that,

$$\begin{aligned} gg^{-1} = 1_{\mathcal{G}} &= g^{-1}g \\ \Rightarrow 1_{\mathcal{H}} &= \varphi(g)\varphi(g^{-1}) \\ &= \varphi(g^{-1})\varphi(g). \end{aligned}$$

Hence,

$$\varphi(g^{-1}) = \varphi(g)^{-1}.$$

□

Definition 3.52 (kernel)**.** If $\varphi : \mathcal{G} \to \mathcal{H}$ is a group homomorphism, then the *kernel* is the set $\ker(\varphi) = \{g \in \mathcal{G} : \varphi(g) = e_h \in \mathcal{H}\}$.

If $\varphi : \mathcal{G} \to \mathcal{H}$ is a group homomorphism, then observe that $\ker(\varphi)$ is a normal subgroup of of $\mathcal{G}$.

3.8. **Characters.** A *group character* is a group homomorphism, $\chi : \mathcal{G} \to \mathbb{C}^{\times}$, from a finite abelian group to the multiplicative group of nonzero complex numbers. In particular;

Definition 3.53 (Character)**.** Let $\mathcal{G}$ be a finite abelian group of order n, written additively. A *character* of $\mathcal{G}$ is a group homomorphism, $\chi : \mathcal{G} \to \mathbb{C}^{\times}$, of $\mathcal{G}$, that is:

$$\chi(g_1 + g_2) = \chi(g_1)\chi(g_2) : g_1, g_2 \in \mathcal{G}.$$

Lemma 3.54.

$$\begin{aligned} \chi(g)^n &= \chi(ng) \\ &= \chi(0) = 1 : g \in \mathcal{G}. \end{aligned}$$

Hence the values of χ are the n^{th} roots of unity.

Lemma 3.55.

$$\begin{aligned} \chi(-g) &= \chi(g)^{-1} \\ &= \overline{\chi(g)} \end{aligned}$$

where the bar denotes the complex conjugation.

Definition 3.56 (Principle Character)**.** The *principle character*, denoted by χ_0, is defined by

$$\chi_0(g) \doteq 1 : g \in \mathcal{G}.$$

Proposition 3.57. *For any non-principle character χ of $\mathcal{G}$,*

$$\sum_{g \in \mathcal{G}} \chi(g) = 0.$$

Proof. Let $h \in \mathcal{G} : \chi(h) \neq 1$ and let $S = \sum_{g \in \mathcal{G}} \chi(g)$. Then,

$$\begin{aligned} \chi(h) \cdot S &= \chi(h) \sum_{g \in \mathcal{G}} \chi(g) \\ &= \sum_{g \in \mathcal{G}} \chi(h)\chi(g) \\ &= \sum_{g \in \mathcal{G}} \chi(g+h) \\ &= S. \end{aligned}$$

Hence it follows that,

$$\begin{aligned} \chi(h) \cdot S &= S \\ (\chi(h) - 1) \cdot S &= 0 \end{aligned}$$

and since $\chi(h) \neq 1$ then,

$$\Rightarrow S = 0.$$

□

Corollary (First orthogonality relation for characters)**.** *Let χ and ψ be two characters of $\mathcal{G}$. Then*

$$\sum_{g \in \mathcal{G}} \overline{\chi(g)}\psi(g) = \begin{cases} n & \text{if } \chi = \psi, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Consider the two cases.

i.) For when $\chi = \psi$ it is trivially so, by that,

$$\begin{aligned} \overline{\chi(g)} &= \chi(g)^{-1} \\ \Rightarrow \overline{\chi(g)}\chi(g) &= 1 \qquad \text{(for each } g \in \mathcal{G}) \end{aligned}$$

and that $|\mathcal{G}| = n$.

ii.) If $\chi \neq \psi$ then $\overline{\chi}\psi$ is a non-principle character and so $\overline{\chi(g)}\psi(g) = 0$ for each $g \in \mathcal{G}$. □

Remark. As observed in the last proof, the point wise product of the characters χ and ψ is again a character:

$$(\chi\psi)(g) \doteq \chi(g)\psi(g).$$

Problem 3.58. *Let $\widehat{\mathcal{G}}$ denote the set of characters. Check that $\widehat{\mathcal{G}}$ forms an abelian group under the operation defined by $(\chi\psi)(g) \doteq \chi(g)\psi(g)$ for every $g \in \mathcal{G}$. We call $\widehat{\mathcal{G}}$ the* dual group *of $\mathcal{G}$.*

Proposition 3.59. *Let ω be a* primitive *n^{th} root of unity. Then the map $\chi_j : \mathbb{Z}_n \to \mathbb{C}^\times$ defined by $\chi_j(k) = \omega^{kj} : k \in \mathbb{Z}_n$ is a character of $\mathbb{Z}_n$ for every $j \in \mathbb{Z}$. Moreover,*

(1) $\chi_i = \chi_j \Leftrightarrow i \equiv j \pmod n$;
(2) $\chi_j = \chi_1^j$;
(3) $\widehat{\mathbb{Z}_n} = \{\chi_0, \dots, \chi_{n-1}\}$;
(4) Consequently, $\widehat{\mathbb{Z}_n} \cong \mathbb{Z}_n$.

Proof. TODO.. □

Proposition 3.60. *If $\mathcal{G}$ is a direct sum, $\mathcal{G} = H_1 \oplus H_2$, and $\psi_i : H_i \to \mathbb{C}^\times$ is a character of H_i, with $i \in \{1, 2\}$, then $\chi = \psi_1 \oplus \psi_2$, defined by*

$$\chi(h_1, h_2) \doteq \psi_1(h_1) \cdot \psi_2(h_2),$$

is a character of $\mathcal{G}$. Moreover, all characters of $\mathcal{G}$ are of this form. Consequently,

$$\widehat{\mathcal{G}} = \widehat{H_1} \oplus \widehat{H_2}.$$

Proof. TODO.. □

Corollary.

$$\widehat{\mathcal{G}} \cong \mathcal{G}.$$

Proof.

Observe that,

$$\begin{aligned} \mathcal{G} &\cong \mathbb{Z}_{n1} \oplus \cdots \oplus \mathbb{Z}_{nk} \\ \Rightarrow \widehat{\mathcal{G}} &\cong \widehat{\mathbb{Z}_{n1}} \oplus \cdots \oplus \widehat{\mathbb{Z}_{nk}} \\ &\cong \mathcal{G}. \end{aligned}$$

□

3.9. **Cosets.** Let $\mathcal{G}$ be a group and $\mathcal{H}$ be a subgroup of $\mathcal{G}$ with $g \in \mathcal{G} : g \notin H$, then

Definition 3.61 (Left Coset)**.** $gH = \{gh : h \in H\}$ is a **left coset of** $\mathcal{H}$ in $\mathcal{G}$.

Definition 3.62 (Right Coset)**.** $Hg = \{hg : h \in H\}$ is a **right coset of** $\mathcal{H}$ in $\mathcal{G}$.

Definition 3.63 (Normal Subgroup)**.** If $gH = Hg$ then $\mathcal{H}$ is a **normal** subgroup of $\mathcal{G}$, denoted by $\mathcal{H} \trianglelefteq \mathcal{G}$.

Theorem 3.64 (Lagrange's Theorem)**.** *TODO.*

Proof. TODO. □

3.10. **Factor (or Quotient) groups.** Let $\mathcal{G}$ be a commutative group and consider a subgroup $\mathcal{H}$. Then $\mathcal{H}$ determines an equivalence relation in $\mathcal{G}$ given by

$$x \sim x' \text{ iff } x - x' \in \mathcal{H}.$$

..

3.11. **Non-commutative Groups.** A common class of non-commutative groups are transformation groups. Note:

Definition 3.65 (Transformation)**.** A bijective map $\varphi : X \to X$ is called a **transformation** of X.

Note. The most trivial case is the *idenitity map* id_X by $id_X(x) = x$, $\forall x \in X$.

Hence, there exists a inverse φ^{-1} of φ such that $\varphi^{-1} \circ \varphi = id_X = \varphi \circ \varphi^{-1}$. Now, take two transformations of X, φ and ψ, and let the product $\varphi \circ \psi$ be well defined. Then the set of all transformations of X form the group **Transf(X)**. Since, given $\varphi, \psi, \phi \in Transf(X)$ then we have associativity, $\varphi \circ (\psi \circ \phi) = (\varphi \circ \psi) \circ \phi$. We have identity $e = id_X \in Transf(X)$ and so, inverses $\forall \varphi \in Transf(X) \exists! \varphi^{-1} : \varphi \circ \varphi^{-1} = e$. Closure follows from the composition of two transformations φ and ψ, since $(\varphi \circ \psi)^{-1} = \psi^{-1} \circ \varphi^{-1}$.

A transformation group is a type of group action which describes symmetries of objects. More abstractly, since a group $\mathcal{G}$ is a category with a single object in which every morphism is bijective. Then, a group action is a *forgetful functor* $\mathcal{F}$ from the group $\mathcal{G}$ in the category **Grp** to the set category **Set** that is, $\mathcal{F} : \mathcal{G} \to \textbf{Set}$.

3.12. **Exact sequence.** An **exact sequence** may either be a finite or infinite sequence of objects and morphisms between them. Such a sequence is constructed so that the image of one morphism equals the kernel of the next.

In particular;

Definition 3.66 (Exact Sequence)**.** Consider the sequence of n group homomorphism between $n + 1$ groups in the following way:

$$\mathcal{G}_0 \xrightarrow{\varphi_1} \mathcal{G}_1 \xrightarrow{\varphi_2} \mathcal{G}_2 \xrightarrow{\varphi_3} \dots \xrightarrow{\varphi_n} \mathcal{G}_n$$

Then the sequence is said to be *exact* if,

$$\ker(\varphi_{k+1}) = \operatorname{im}(\varphi_k)$$

for every $k \in \{1 \dots n\}$. For $n = 3$ the sequence is said to be a **short exact sequence**.

Example 3.67. Suppose we have $\mathcal{K} \trianglelefteq \mathcal{G}$ and that $q : \mathcal{G} \to \mathcal{G}/\mathcal{K}$ is the quotient mapping. Then,

$$1 \longrightarrow \mathcal{K} \xrightarrow{\subseteq} \mathcal{G} \xrightarrow{q} \mathcal{G}/\mathcal{K} \longrightarrow 1$$

is a short exact sequence.

4. First Isomorphism Theorem

Theorem 4.1. *Let $\mathcal{G}$ and $\mathcal{H}$, and let $\varphi : \mathcal{G} \to \mathcal{H}$ be a group homomorphism. Then:*

- *The kernel of φ is a normal subgroup of $\mathcal{G}$; $\ker(\varphi) \trianglelefteq \mathcal{G}$,*
- *The image of φ is a subgroup of $\mathcal{H}$; $\operatorname{im}(\varphi) \leq \mathcal{H}$, and*
- *The image of φ is also isomorphic to the factor group $\mathcal{G}/\ker(\varphi)$; $\operatorname{im}(\varphi) \cong \mathcal{G}/\ker(\varphi)$.*

In particular, if φ is epimorphic then $\mathcal{H} \cong \mathcal{G}/\ker(\varphi)$.

We may represent these fundamental relations in the following commutative diagram.

$$\begin{tikzcd}
 & & 0 \arrow[dr] & & 0 \\
 & & & \begin{array}{c}\mathcal{G}/\ker(\varphi) \\ \scriptstyle\cong \operatorname{im}(\varphi)\end{array} \arrow[ur] \arrow[dr, "\iota"] & \\
 & & \mathcal{G} \arrow[ur, "\pi"] \arrow[rr, "\varphi"] & & \mathcal{H} \\
 & \ker(\varphi) \arrow[ur, "\kappa"] & & & \\
0 \arrow[ur] & & & &
\end{tikzcd}$$

Notice the *exact sequence* that runs from the lower left to the upper right of the commutative diagram.