Chapter 1

Groups

Lectured by Dr Michele Zordan
Typed by Yu Coughlin
Spring 2024

Introduction

Lecture 1
Thursday
10/01/19

The following are supplementary reading:

- J B Fraleigh, A first course in abtract algebra, 2014
- R B J T Allenby, Rings, field and groups: an introduction to abstract algebra, 1991
- A W Knapp, Basic Algebra, 2006

Contents

1 Binary operations and groups

Definition 1.0.1 (Binary operation)**.** Given a set G a **binary operation** on G is a mapping $\cdot : G \times G \to G$ written $\cdot(g, h) = g \cdot h$ (and sometimes gh) for all $g, h \in G$.

Definition 1.0.2 (Group)**.** A **group** is a pair $G = (G, \cdot)$, for some set G and a binary operation $\cdot$, satisfying the following properties:

(G1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$ (the binary operation is **associative**),

(G2) $\exists e \in G$ such that $\forall g \in G g \cdot e = e \cdot g = g$ (there is an **identity** element),

(G3) $\forall g \in G, \exists g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$ (every element has an **inverse**).

In some literature, the condition of **closure** is also required however this is given in the fact that $\cdot$ is a binary operation on G.

Theorem 1.0.3 (Uniqueness of identity)**.** The identity element for some group G is unique. The inverse, g^{-1}, of any element $g \in G$ is also unique.

Proof. Given identities $e_1, e_2 \in$ G, $e_1 = e_1 \cdot e_2 = e_2$. □

Lemma 1.0.4 (Inverse of product)**.** Given a group G and the elements $g_1, g_2, \ldots, g_n \in G$ we have,

$$(g_1 g_2 \ldots g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}.$$

Proof. $(g_1 g_2 \ldots g_n)(g_n^{-1} \ldots g_2^{-1} g_1^{-1}) = e$ clearly, so $(g_1 g_2 \ldots g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$. □

Lemma 1.0.5 (Uniquess of inverses)**.** The inverse of an element $g \in G$ is unique.

Proof. Suppose a, b are inversers of $g \in G$, $ag = e = bg \Rightarrow a = b$. □

Definition 1.0.6 (Abelian Group)**.** If a group G also satisfies the condition $g \cdot h = h \cdot g$ for all $g, h \in G$ (**commutativity**), then G is an **abelian group**.

Definition 1.0.7 (Powers of elements)**.** Given a group G and some $g \in G$ the nth **power** of g in G is defined recursively as,

$$g^n := \begin{cases} \text{e} & \text{if } n = 0 \\ g^{n-1} g & \text{if } n > 0 \\ (g^n)^{-1} & \text{if } n < 0 \end{cases}.$$

Definition 1.0.8 (Order of group)**.** The **order** of a group G, written $|G|$, is the cardinality of the set of G.

Example 1.0.9 (Symmetric group)**.** The **symmetric group of size** n, denoted S_n, is the set of bijections on the interval $[1, n]$, for $n \in \mathbb{N}$, under function composition. In generarl, given a set X, $\text{Sym}(X)$ is the group of permutations of X.

2 Subgroups

2.1 Subgroups

Definition 2.1.1 (Subgroup)**.** Given a group $(G, \cdot)$ and a subset $H \subseteq G$ we say $(H, \cdot)$ is a **subgroup** of G, written $H \leq G$, if $(H, \cdot)$ is a group. H is a **proper subgroup** iff $H \neq G$.

Theorem 2.1.2 (Subgroup test)**.** Given a group $(G, \cdot)$, $(H, \cdot)$ is a subgroup iff:

(S1) H is non-empty (**existence**),

(S2) for all $h_1, h_2 \in H$ we have $h_1 \cdot h_2 \in H$ (**closure under group operation**),

(S3) for all $h \in H$ we have $h^{-1} \in H$ (**closure under inverses**).

Proof. ($\Leftarrow$) is simple. For ($\Rightarrow$): group axioms $\Rightarrow$ (S1) and (S2), as H is a group, h must have an inverse $h' \in H$, inverses are unique $\Rightarrow$ (S3). □

2.2 Cyclic groups and orders

Definition 2.2.1 (Cyclic group)**.** We say a group G is **cyclic** if there is an element $g \in G$ such that

$$G = \langle g \rangle := \{g^n : n \in \mathbb{N}\}.$$

We say that G is **generated** by g or g is a **generator** of G.

Definition 2.2.2 (Order of elements)**.** Given a group G and some $g \in G$, the **order** of g in G, written $\operatorname{ord} g$, is the smallest positive integer n such that $g^n = e$ or ∞ if no such n exists.

Theorem 2.2.3. Suppose G is a group with $g \in G$ having finite order n, $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$.

Lemma 2.2.4. For $a, b \in \mathbb{Z}$, $g^a = g^b \;\Leftrightarrow\; a \equiv b \pmod n$

Proof. ($\Leftarrow$) is simple. For ($\Rightarrow$), $g^a = g^b \;\Rightarrow\; g^{a-b} = e$, by division algorithm $\Rightarrow\; e = g^{qn+r} = (g^n)^q \cdot g^r = g^r$ so $r = 0$ and $n|a-b$. □

Proof of 2.2.3. All $m \in \mathbb{Z}$ are congruent to one of $0, 1, \dots, n-1 \pmod n$ so $\langle g \rangle = \{g^m : m \in \mathbb{Z}\} = \{e, g, \dots, g^{n-1}\}$. □

Theorem 2.2.5. Suppose G is a cyclic group with $G = \langle g \rangle$, the three statements:

1. $H \leq G \;\Rightarrow\; H$ is cyclic,
2. suppose $|G| = n$ and $m \in \mathbb{Z}$ with $d = \gcd(m, n)$,
$$\langle g^m \rangle = \langle g^d \rangle \text{ and } |\langle g^m \rangle| = \frac{n}{d}.$$
In particular, $\langle g^m \rangle = G$ iff $\gcd(m, n) = 1$,
3. if $|G| = n$ and $k \leq n$, then G has a subgroup of order k iff $k|n$, this subgroup is $\langle g^{n/k} \rangle$.

Proof.

1. Have $H \neq \{e\}$, consider $d := \min\{n \in \mathbb{N} : g^n \in H\}$, clearly $\langle g^d \rangle \leq H$. For all $h = g^m \in H$, $g^m = g^{pd+r} = (g^d)^p \cdot g^r \;\Rightarrow\; g^r = h(g^d)^{-p} \in H$ therefore $r = 0$ so $h \in \langle g^d \rangle$ and $H = \langle g^d \rangle$.
2. ($\subseteq$) $g^d = g^{km} \in \langle g^m \rangle$. ($\supseteq$) Have $d = am + bn$ (Bézout's identity), $g^d = g^{am+bn} = g^{am}g^{bn} = (g^m)^a \in \langle g^d \rangle$.
3. ($\Rightarrow$) 1. ($\Leftarrow$) 2.

□

Definition 2.2.6 (Euler totient)**.** The **Euler totient** function ϕ is defined as $\phi(n) := |\{k \in \mathbb{N} : k \leq n \text{ and } \gcd(k, n) = 1\}|$.

Corollary 2.2.7. For $n \in \mathbb{N}$:
$$\sum_{d|n} \phi(d) = n.$$

Proof. Consider the cyclic group of order n, G. If $d|n$, $\langle g^{n/k} \rangle$ is the subgroup with all elements of order d with $\phi(d)$ elements of order d. By summing this for $d|n$ (orders of elements in G) we count all of the n elements of G by their order. □

2.3 Cosets

Definition 2.3.1 (Coset)**.** Given a group G with $H \leq G$ and $g \in G$ then

$$gH := \{gh : h \in H\},$$

is a **left coset** of H in G (similarly for a **right cosets**). We will now assume all **cosets** to be left cosets.

Lemma 2.3.2. Given a group G with $H \leq G$, all cosets of H in G have the same size.

Proof. Lemma 3.0.4 $\Rightarrow$ $|H| = |gH|$ for all $g \in G$. □

Lemma 2.3.3. If G is a finite group with $H \leq G$, the cosets of H form a partition of G.

Proof.

1. If $g_1 \in g_2H$ (by h), for some $g_1h' \in g_1H$, $g_1h' = g_2(hh') \in g_2H$, $g_2 = g_1h^{-1} \in g_1H$.
2. If $x \in g_1H \cap g_2H$ ($g_1H \cap g_2H \neq \emptyset$), apply 1. twice to get $g_1H = xH = g_2H$.

□

2.4 Lagrange's theorem

Theorem 2.4.1 (Lagrange's theorem)**.** If G is a finite group and $H \leq G$, $|H|$ divides $|G|$.

Proof. Partition G into the $n \in \mathbb{N}$ distinct cosets of H all with size $|H|$, $|G| = n|H|$. Have $n := [G : H]$. □

Corollary 2.4.2. Given a group G with $H \leq G$, the relation $\sim$ on G given by: $g \sim k$ iff $g^{-1}k \in H$, is an equivalence relation with equivalence classes given by cosets of H.

Proof. $g \sim k \;\Rightarrow\; k \in gH$ equivalence relation from partition (IUM part 1) given by cosets of G by H. □

Corollary 2.4.3. Given a group G of order n, for all $g \in G$, $\operatorname{ord} g | n$ and $g^n = e$.

Proof. Apply Lagrange's theorem with $H = \langle g \rangle$, $g^n = (g^{\operatorname{ord} g})^{n/\operatorname{ord} g} = e^{n/\operatorname{ord} g} = e$ (due to first part). □

Corollary 2.4.4 (Fermat's little theorem)**.** Let p be prime. If $x \in \mathbb{Z}$ and $p \nmid x$, then $x^{p-1} \equiv 1 (\text{mod } p)$.

Proof. Let $G = (\mathbb{Z}/p\mathbb{Z})^*$, $|G| = p - 1$ and (by Corollary 2.4.3) $[x^{p-1}] = [x]^{p-1} = [1]$ for all $[x] \in G$. □

Corollary 2.4.5. If a group G is of prime order, G is cyclic and $\langle g \rangle = G$ for all $(g \neq e) \in G$.

Proof. By Lagrange's Theorem $|\langle g \rangle|$ divides p, as $g \neq e$, $|\langle g \rangle| = p \;\Rightarrow\; \langle g \rangle = G$. □

2.5 Generating groups

Definition 2.5.1. Given a group G with $S \subseteq G$, $S^{-1} := \{g^{-1} \in G : g \in S\}$.

Definition 2.5.2 (Subgroup generated by a set)**.** Let G be a group with non-empty $S \subseteq G$. The **subgroup generated by** S is defined as

$$\langle S \rangle := \{g_1 g_2 \dots g_k \in G : k \in \mathbb{N} \text{ and } g_i \in S \cup S^{-1} \text{ for all } i \in [1, k]\}.$$

Lemma 2.5.3. Given a group G with non-empty $S \subseteq G$, $\langle S \rangle \leq G$ and, $H \leq G,\; S \subseteq H \;\Rightarrow\; \langle S \rangle \leq H$. This is equivalent to saying "$\langle S \rangle$ is the smallest subgroup of G containing S".

Proof. □

3 Group homomorphisms

Definition 3.0.1 (Group homomorphism)**.** If $(G, \cdot)$ and $(H, *)$ are goups, $\phi : G \to H$ is a **group homomorphism** iff $\phi(g_1) * \phi(g_2) = \phi(g_1 \cdot g_2)$ for all $g_1, g_2 \in G$. If ϕ is bijective then it is called a **group isomorphism** with G and H being **isomorphic**, written $G \cong H$.

Example 3.0.2 (determinant)**.** The **determinant** is a group homomorphism, suppose $\mathbb{F}$ is a field:

$$\det : \mathrm{GL}(n, \mathbb{F}) \to (\mathbb{F}^*, \times).$$

Lemma 3.0.3. If G,H are groups with $\phi : G \to H$,

1. $\phi(e_G) = e_H$,
2. $\phi(g^{-1})(\phi(g))^{-1}$ for all $g \in G$.

Proof.
1. $\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G) \;\Rightarrow\; \phi(e_G) = e_H$.
2. $e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$. □

Lemma 3.0.4 (Isomorphism from group operation)**.** Given g in the group G, $\phi_g : G \to G$ given by $\phi_g : x \mapsto gx$ is an isomorphism (same for right multiplication).

Proof. injectivity: $\phi_g(x) = \phi_g(y) \;\Rightarrow\; gx = gy \;\Rightarrow\; x = y$, surjectivity: given $x \in G$, $\phi_g(g^{-1}x) = x$. □

Definition 3.0.5 (Image and kernel of group homomorphism)**.** If G,H are groups with $\phi : G \to H$, the **image** of ϕ is:

$$\operatorname{im} \phi := \{h \in H : \exists g \in G, h = \phi(g)\}.$$

and the **kernel** of ϕ is

$$\ker \phi := \{g \in G : \phi(g) = e_H\}.$$

These are each subgroups of H and G respectively.

Lemma 3.0.6. A group homomorphism, $\phi : G \to H$, is injective iff $\ker\phi = \{e_H\}$.

Proof. ($\Rightarrow$) $\phi(g) = e_H = \phi(e_G)$ so $g = e_G$ and $\ker\phi = \{e_G\}$.

($\Leftarrow$) Supposing $\phi(g_1) = \phi(g_2)$, $\phi(g_1g_2^{-1}) = e_H \Rightarrow g_1g_2^{-1} \in \ker\phi = \{e_G\}$ therefore $g_1 = g_2$. □

Theorem 3.0.7. The composition of two compatible group homomorphisms is also a group homomorphism.

Proof. Have groups G, H, J with homomorphisms $\phi : G \to H, \psi : H \to J$, $\psi(\phi(g_1g_2)) = \psi(\phi(g_1)\phi(g_2)) = \psi(\phi(g_1))\psi(\phi(g_2))$. □

Theorem 3.0.8. All cyclic groups of the same order are isomorphic.

Proof. Have $G = \langle g\rangle$ and $H = \langle h\rangle$ both order n with $\phi : G \to H$, $\phi : g^k \mapsto h^j$, one can be clearly show, with Lemma 2.2.4, ϕ is an isomorphism. □

4 Symmetric groups

4.1 Disjoint cycle decomposition

Definition 4.1.1. If $f, g \in S_n$ and $x \in [1, n]$ then f **fixes** x if $f(x) = x$ and f **moves** x otherwise.

Definition 4.1.2. The **support** of $f \in S_n$ is the set of points f moves, $\mathrm{supp}(f) := \{x \in [1, n] : f(x) \neq x\}$.

Definition 4.1.3. If $f, g \in S_n$ satisfy $\mathrm{supp}(f) \cap \mathrm{supp}(g) = \emptyset$, f and g are **disjoint**.

Lemma 4.1.4. If $f, g \in S_n$ are disjoint, $fg = gf$.

Proof. For all $x \in [1, n]$ if x is fixed by both f and g we are done, otherwise wlog have f fix $x \Rightarrow x \neq g(x) \neq g(g(x))$ so $g(x) \in \mathrm{supp}(g) \Rightarrow g(x) \notin \mathrm{supp}(f)$ giving $f(g(x)) = g(x) = g(f(x))$. □

Definition 4.1.5 (Cycles)**.** If $f \in S_n$ with $i_1, i_2, \ldots, i_r \in [1, n]$ for some $r \leq n$ such that,

$$f(i_s) = i_{s+1 \pmod{} r} \text{ for all } s \in [1, r],$$

with f fixing all other elements of $[1, n]$, then f is a **cycle of length** r or an r**-cycle** and we write $f = (i_1i_1 \ldots i_r)$.

Theorem 4.1.6 (Disjoint cycle form)**.** if $f \in S_n$ then there exists $f_1, f_2, \ldots, f_k \in S_n$ all with disjoint supports such that $f = f_1f_2 \ldots f_n$. If we further have, for all $i \in [1, k]$, both f_i is not a 1-cycle when $f \neq \mathrm{id}$ and $\mathrm{supp}(f_i) \subseteq \mathrm{supp}(f)$. We say f is in **disjoint cycle form** or **d.c.f**.

Proof. We use strong induction on $m := |\mathrm{supp}(f)|$. If $m = 0$: $f = \mathrm{id}$. If, instead, $m \geq 1$: have some $i_1 \in \mathrm{supp}(f)$ and set $f(i_1) = i_2, f(i_2) = i_3, \ldots$ with i_r being the first satisfying $f(i_r) \in \{i_1, i_2, \ldots i_{r-1}\}$, due to bijectivity of f, $f(i_r) = i_1$ we can now have $f = gf_1$ where $f_1 = (i_1i_2 \ldots i_r)$ with $|\mathrm{supp}(g)| < m$ so, inductively, f can be decomposed into disjoint cycles. □

Theorem 4.1.7 (Uniqueness of disjoint cycles)**.** The disjoint cycle form of some $f \in S_n$ is unique up to rearrangement.

Proof. Have $f \in S_n$ with $g_1g_2 \ldots g_k = f = h_1h_2 \ldots h_l$ by rearring f and individul cycles have $i_1 \in f_k$ and $i_1 \in h_l$ with $r \in \mathbb{N}$ the minimum value with $f^r(i_1) = i_1$. $g_k = (i, f(i), f^2(i), \ldots, f^{r-1}(i)) = h_l \Rightarrow g_1g_2 \ldots g_{k-1} = h_1h_2 \ldots h_{l-1}$ so, by induction, $l = k$ and $g_i = h_i$ for all $i \in [1, k]$ $\therefore$ dcf is unique. □

Theorem 4.1.8. If $f \in S_n$ is written in d.c.f as $f = f_1f_2 \ldots f_k$ where f_i is an r_i-cycle for $i \in [1, k]$ then,

1. $f^m = \mathrm{id}$ iff $f_i^m = \mathrm{id}$ for all $i \in [1, k]$,
2. $\mathrm{ord}(f) = \mathrm{lcm}(r_1, r_2, \ldots r_k)$.

Proof.
1. ($\Rightarrow$) $f_1^mf_2^m \ldots f_k^m = id$ and f_i^m having disjoint supports $\Rightarrow f_i^m(x) = x$ so $f_i^m = \mathrm{id}$. ($\Leftarrow$) product of identites is the identity.
2. $f^m = \mathrm{id} \Leftrightarrow f_i^m = \mathrm{id} \Leftrightarrow r_i|m$, the least m satisfying this for all r_i is $\mathrm{lcm}(r_1, r_2, \ldots, r_i)$. □

4.2 Alternating groups

Theorem 4.2.1. Every permutation in S_n can be written as the product of 2-cycles.

Proof. $(a_1 a_2 \dots a_n) = (a_1 a_2)(a_2 a_3) \cdots (a_{n-1} a_n)$. □

Definition 4.2.2 (Sign of a permutation)**.** We define the **sign** of a permutation with the group homomorphism, $\mathrm{sgn} : S_n \to \{-1, 1\}$ with $\mathrm{sgn}(i\ j) := -1$ for all $i, j \in [1, n]$ with $i \neq j$. This is defined over all permutations by the decomposition into 2-cycles, the sign of a permutation is unique. We say $f \in S_n$ is **even** if $f \in \ker(\mathrm{sgn})$ and **odd** otherwise.

Definition 4.2.3 (Alternating group)**.** The **alternating group** of size n is $A_n := \ker(\mathrm{sgn})$ with $A_n \leq S_n$.

4.3 Dihedral groups

Definition 4.3.1 (Dihedral group)**.** The **dihedral group** of order $2n$, denoted D_{2n}, is the group of symmetries of a regular n-gon in $\mathbb{R}^3$ centered at the origin, it is often written at

$$D_{2n} = \{e, r, r^2, \dots, r^{n-1}, s, sr, sr^2 \dots, sr^{n-1}\},$$

where r is a rotation by $\frac{2\pi}{n}$ and s is the reflection along the centre of the polygon and the first vertex.

Theorem 4.3.2. The elements of D_{2n} can be written as elements of S_n giving $D_{2n} \leq S_n$. Specifically, $r = (1\ 2\ \dots\ n)$ and $s = (1)(2\ n)(3\ n-1)\dots$ or $(1\ n)(2\ n-1)\dots$ if n is odd or even respectively.

Proof. Given in definition. □

5 Group-like objects*

Definition 5.0.1 (Group-like objects)**.** There are multiple axioms in the defintion of a group, sometimes we are interested in objects which lack some / all of these axioms; the names of said objects are: