Group Theory

J. S. Milne

January 9, 2022

Contents

1 Basic Definitions and Results

1.1 Definitions and examples

The **order** $|G|$ of a group is its cardinality. A finite group whose order is a power of a prime p is called a p**-group**

C_n denote any cyclic group of order n

Example 1.1. Let V be a finite-dimensional vector space over a field F. A bilinear form on V is a mapping $\phi : V \times V \to F$ that is linear in each variable. An **automorphism** of such a ϕ is an isomorphism $\alpha : V \to V$ s.t.

$$\phi(\alpha v, \alpha w) = \phi(v, w) \text{ for all } v, w \in V$$

The automorphism of ϕ form a group Aut(ϕ). Let $\{e_1, \dots, e_n\}$ be a basis for V, and let

$$P = (\phi(e_i, e_j))_{1 \leq i,j \leq n}$$

be the matrix of ϕ. The choice of the basis identifies Aut(ϕ) with the group of invertible matrices A s.t.

$$A^T \cdot P \cdot A = P$$

When ϕ is symmetric, i.e.,

$$\phi(v, w) = \phi(w, v) \text{ all } v, w \in V$$

and nondegenerate, Aut(ϕ) is called the **orthogonal group** of ϕ

Theorem 1.1 (Cayley)**.** *There is a canonical injective homomorhism*

$$\alpha : G \to \mathrm{Sym}(G)$$

Corollary 1.2. *A finite group of order n can be realized as a subgroup of S_n*

Proposition 1.3. *Let H be a subgroup of a group G*

1. *An element $a \in G$ lies in a left coset C of H iff $C = aH$*
2. *Two left cosets are either disjoint or equal*
3. *$aH = bH$ iff $a^{-1}b \in H$*
4. *Any two left cosets have the same number of elements*

The **index** $(G : H)$ of H in G is defined to be the number of left cosets of H in G. For example, $(G : 1)$ is the order of G

Theorem 1.4 (Lagrange)**.** *If G is finite, then*

$$(G : 1) = (G : H)(H : 1)$$

Proof. The left cosets of H in G form a partition of G, there are $(G : H)$ of them □

Corollary 1.5. *The order of each element of a finite group divides the order of the group*

Proof. Consider $H = \langle g \rangle$ $\square$

Proposition 1.6. *For any subgroups $H \supset K$ of G*

$$(G : K) = (G : H)(H : K)$$

Proof. $G = \coprod_{i \in I} g_i H$, and $H = \coprod_{j \in J} h_j K$ $\square$

1.2 Normal subgroups

A subgroup N of G is **normal**, denoted $N \lhd G$, if $gNg^{-1} = N$ for all $g \in G$ it suffices to check that $gNg^{-1} \subset N$

Proposition 1.7. *subgroup N of G is normal iff every left coset of N in G is also a right coset*

Example 1.2. 1. Every subgroup of index two is normal. Indeed, let $g \in G \setminus H$, then $G = H \coprod gH = H \coprod Hg$

A group G is **simple** if it has no normal subgroups other than G and $\{e\}$.

Proposition 1.8. *If H and N are subgroups of G and N is normal, then HN is a subgroup of G. If H is also normal, then HN is a normal subgroup of G*

Intersection of normal subgroups of a group is again a normal subgroup. Therefore we can define the **normal subgroup generated by a subset** X of a group G to be the intersection of the normal subgroups containing X. We say that a subset X of a group G is **normal** if $gXg^{-1} \subset X$ for all $g \in G$

Lemma 1.9. *If X is normal, then the subgroup $\langle X \rangle$ generated by it is normal*

Lemma 1.10. *For any subset X of G, the subset $\bigcup_{g \in G} gXg^{-1}$ is normal, and it is the smallest normal set containing X*

Proposition 1.11. *The normal subgroup generated by a subset X of G is $\langle \bigcup_{g \in G} gXg^{-1} \rangle$*

Proposition 1.12. *The map $a \mapsto aN : G \to G/N$ has the following universal property: for any homomorhism $\alpha : G \to G'$ of groups s.t. $\alpha(N) = \{e\}$, there exists a unique homomorhism $G/N \to G'$ making the diagram*

$$\begin{tikzcd} G \arrow[r, "a\mapsto aN"] \arrow[dr, "\alpha"'] & G/N \arrow[d, dashed] \\ & G' \end{tikzcd}$$

commute

Proof. Define $\bar{\alpha} : G/N \to G'$, $\bar{\alpha}(gN) = \alpha(g)$ $\square$

1.3 Theorems concerning homomorhisms

The kernel of the homomorhism $\det : \mathrm{GL}_n(F) \to F^\times$ is the group of $n \times n$ with determinant 1 - this group $\mathrm{SL}_n(F)$ is called the **special linear group of degree** n

Theorem 1.13 (HOMOMORPHISM THEOREM)**.** *For any homomorhism $\alpha : G \to G'$ of groups, $\ker\alpha \lhd G$, $\operatorname{im}\alpha \leq G'$, and α factors in a natural way into the composite of a surjection, an isomorphism, and an injection*

$$\begin{tikzcd} G \arrow[r, "\alpha"] \arrow[d, two heads, "g\mapsto gN"] & G' \\ G/N \arrow[r, "\sim", "gN\mapsto\alpha(g)"'] & I \arrow[u, hook] \end{tikzcd}$$

Theorem 1.14 (ISOMORPHISM THEOREM)**.** *$H \leq G$, $N \lhd G$. Then $HN \leq G$, $H \cap N \lhd G$*

$$h(H \cap N) \mapsto hN : H/H \cap N \to HN/N$$

is an isomorphism

link
$\overline{G}$ is a quotient group of G

Theorem 1.15 (CORRESPONDENCE THEOREM)**.** *Let $\alpha : G \twoheadrightarrow \overline{G}$ be a surjective homomorhism, and let $N = \ker\alpha$. Then there is a one-to-one correspondence*

$$\{\textit{subgroups of } G \textit{ containing } N\} \leftrightarrow \{\textit{subgroups of } \overline{G}\}$$

under which a subgroup H of G containing N corresponds to $\overline{H} = \alpha(H)$ and a subgroup $\overline{H}$ of $\overline{G}$ corresponds to $H = \alpha^{-1}(\overline{H})$. Moreover, if $H \leftrightarrow \overline{H}$ and $H' \leftrightarrow \overline{H}'$, then

1. *$\overline{H} \subset \overline{H}' \Leftrightarrow H \subset H'$, in which case $(\overline{H}' : \overline{H}) = (H' : H)$*

2. $\overline{H} \lhd \overline{G} \Leftrightarrow H \lhd G$ *, in which case α induces an isomorphism*

$$G/H \xrightarrow{\simeq} \overline{G}/\overline{H}$$

Corollary 1.16. *$N \lhd G$; then there is a one-to-one correspondence between the set of subgroups of G containing N and the set of subgroups of G/N, $H \leftrightarrow H/N$. Moreover $H \lhd G \Leftrightarrow H/N \lhd G/N$, in which case the homomorhism $g \mapsto gN : G \to G/N$ induces an isomorphism*

$$G/H \cong (G/N)/(H/N)$$

1.4 Direct products

Let G be a group, and let $H_1, \dots, H_k$ be subgroups of G. G is a **direct product** of the subgroups H_i if the map

$$(h_1, \dots, h_k) \mapsto h_1 \dots h_k : H_1 \times \cdots \times H_k \to G$$

is an isomorphism of groups

note that if $g = h_1 \dots h_k$ and $g' = h'_1 \dots h'_k$, then

$$gg' = (h_1 h'_1) \dots (h_k h'_k)$$

Proposition 1.17. *A group G is a direct product of subgroups H_1, H_2 iff*

1. $G = H_1 H_2$
2. $H_1 \cap H_2 = \{e\}$
3. *every element of H_1 commutes with every element of H_2*

Proof. 3 shows that $(h_1, h_2) \to h_1 h_2$ is a homomorhism, 2 injective, 1 surjective □

Proposition 1.18. *A group G is a direct product of subgroups H_1, H_2 iff*

1. $G = H_1 H_2$
2. $H_1 \cap H_2 = \{e\}$
3. $H_1, H_2 \lhd G$

Proof. The elements h_1, h_2 of a group commute iff their commutator

$$[h_1, h_2] := (h_1 h_2)(h_2 h_1)^{-1}$$

is e. But

$$(h_1 h_2)(h_2 h_1)^{-1} = h_1 h_2 h_1^{-1} h_2^{-2} = \begin{cases} (h_1 h_2 h_1^{-1}) \cdot h_2^{-1} \\ h_1 \cdot (h_2 h_1^{-1} h_2^{-1}) \end{cases}$$

which is in H_2 because H_2 is normal, and is in H_1 because H_1 is normal $\square$

Proposition 1.19. *A group G is a direct product of subgroups $H_1, \dots, H_k$ iff*

1. $G = H_1 \dots H_k$
2. *for each j,* $H_j \cap (H_1 \dots H_{j-1} H_{j+1} \dots H_k) = \{e\}$
3. $H_1, \dots, H_k \lhd G$

1.5 Commutative groups

Let M be a commute group. The subgroup $\langle x_1, \dots, x_k \rangle$ of M generated by the elements $x_1, \dots, x_k$ consists of the sums $\sum m_1 x_i$, $m_i \in \mathbb{Z}$. A subset $\{x_1, \dots, x_k\}$ of M is a **basis** of M if it generates M and

$$\sum m_i x_i = 0, m_i \in \mathbb{Z} \Longrightarrow m_i x_i = 0 \text{ for every } i$$

then

$$M = \langle x_1 \rangle \oplus \cdots \oplus \langle x_k \rangle$$

Lemma 1.20. *Let $x_1, \dots, x_k$ generate M. For any $c_1, \dots, c_k \in \mathbb{N}$ with* $\gcd(c_1, \dots, c_k) = 1$*, there exist generators $y_1, \dots, y_k$ for M s.t. $y_1 = c_1 x_1 + \cdots + c_k x_k$*

Proof. We argue by induction on $s = c_1 + \cdots + c_k$. The lemma certainly holds if $s = 1$, and so we assume $s > 1$. Then, at least two c_i are nonzero, say, $c_1 \geq c_2 > 0$. Now

- $\{x_1, x_2 + x_1, x_3, \dots, x_k\}$ generates M
- $\gcd(c_1 - c_2, c_2, c_3, \dots, c_k) = 1$
- $(c_1 - c_2) + c_2 + \cdots + c_k < s$

and so, by induction, there exist generators $y_1, \ldots, y_k$ for M s.t.

$$\begin{aligned} y_1 &= (c_1 - c_2)x_1 + c_2(x_1 + x_2) + c_3x_3 + \cdots + c_kx_k \\ &= c_1x_1 + \cdots + c_kx_k \end{aligned}$$

□

Theorem 1.21. *Every finitely generated commutative group M has a basis; hence it is a finite direct sum of cyclic groups*

Proof. Induction on the generators of M.

Among the generating sets $\{x_1, \ldots, x_k\}$ for M with k elements there is one for which the order of x_1 is the smallest possible. We shall show that M is the direct sum of $\langle x_1 \rangle$ and $\langle x_2, \ldots, x_k \rangle$

If M is not the direct sum of $\langle x_1 \rangle$ and $\langle x_2, \ldots, x_k \rangle$, then there exists a relation

$$m_1x_1 + \cdots + m_kx_k = 0$$

with $m_1x_1 \neq 0$. After possibly changing the sign of some of the x_i, we may suppose that $m_1, \ldots, m_k \in \mathbb{N}$ and $m_1 < \text{order}(x_1)$. Let $d = \gcd(m_1, \ldots, m_k) > 0$, and let $c_i = m_i/d$. According to the lemma, there exists a generating set $y_1, \ldots, y_k$ s.t. $y_1 = c_1x_1 + \cdots + c_kx_k$. But

$$dy_1 = m_1x_1 + \cdots + m_kx_k = 0$$

and $d \leq m_1 < \text{order}(x_1)$, and so this contradicts the choice of $\{x_1, \ldots, x_k\}$ □

Corollary 1.22. *A finite commutative group is cyclic if, for each $n > 0$, it contains at most n elements of order dividing n*

Proof. After Theorem 1.21, we may assume that $G = C_{n_1} \times \cdots \times C_{n_r}$ with $n_i \in \mathbb{N}$. If n divides n_i and n_j with $i \neq j$, then G has more than n elements of order dividing n First consider $n = p$, then in C_p there are $p - 1$ elements of order dividing p by Lagrange theorem.

Now consider $n = p_1p_2$. If $(k, p_1p_2) = 1$, then order of k is p_1p_2. Hence there are at least $p_1p_2 - p_1 - p_2 - 1$ elements. Check THIS! Therefore the hypothesis implies that the n_i are relatively prime. Let a_i generate the ith factor. Then $(a_1, \ldots, a_r)$ has order $n_1 \ldots n_r$, and so generates G □

Example 1.3. Let F be a field. The elements of order dividing n in $F^\times$ are the roots of the polynomial $X^n - 1$. Because unique factorization holds in $F[X]$, there are at most n of these, and so corollary shows that every finite subgroup of $F^\times$ is cyclic

Theorem 1.23. *A nonzero finitely generated commutative group M can be expressed*

$$M \approx C_{n_1} \times \cdots \times C_{n_s} \times C_\infty^r$$

for certain integers $n_1, \dots, n_s \geq 2$ and $r \geq 0$. Moreover

1. *r is uniquely determined by M*
2. *the n_i can be chosen so that $n_1 \geq 2$ and $n_1 \mid n_2, \dots, n_{s-1} \mid n_s$, and then they are uniquely determined by M*
3. *the n_i can be chosen to be powers of prime numbers, and then they are uniquely determined by M*

The number r is called the **rank** of M. By r being uniquely determined by M, we mean that two decompositions of M of the form , the number of copies of C_∞ will be the same. The integers in (2) are called the **invariant factors** of M. Statement (3) says that M can be expressed

$$M \approx C_{p_1^{e_1}} \times \cdots \times C_{p_t^{e_t}} \times C_\infty^r, \quad e_i \geq 1$$

for certain prime powers $p_i^{e_i}$, and that the integers $p_1^{e_1}, \dots, p_t^{e_t}$ are uniquely determined by M; they are called the **elementary divisors** of M

Proof. The first assertion is a restatement of Theorem 1.21

1. For a prime p not dividing any of the n_i

   $$M/pM \approx (C_\infty/pC_\infty)^r \cong (\mathbb{Z}/p\mathbb{Z})^r$$

   and so r is the dimension of M/pM as an $\mathbb{F}_p$-vector space suppose $C_n = \langle a \rangle$ and $f : C_n \to pC_n : a \mapsto a^p$. Since $(p, n) = 1$, $|a^p| = n$. Thus this is an isomorphism

2. 3. If $\gcd(m, n) = 1$, then $C_m \times C_n$ contains an element of order mn, and so

   $$C_m \times C_n \approx C_{mn}$$

   In this way we can decomposite C_{n_i} into products of cyclic groups of prime power order. Then we can construct what we want

   To prove the uniqueness of (2) and (3), we can replace M with its torsion subgroup (and so assume $r = 0$).

   uniqueness of elementary divisors is clear.

n_s is the smallest integer > 0 s.t. $n_s M = 0$; n_{s-1}` is the smallest integer > 0 s.t. $n_{s-1}M$ is cyclic; n_{s-2} is the smallest integer s.t. $n_{s-2}M$ can be expressed as a product of two cyclic groups, and so on

in the end, we will get a factoring like

$$
\begin{array}{llll}
C_{p_1^{r_1}} & C_{p_1^{r_2}} & C_{p_1^{r_3}} & C_{p_1^{r_4}} \\
C_{p_2^{s_1}} & C_{p_2^{s_2}} & & \\
C_{p_3^{t_1}} & C_{p_3^{t_2}} & C_{p_3^{t_3}} &
\end{array}
$$

and get out invariant factors

□

1.6 The order of ab

Theorem 1.24. *For any integers $m, n, r > 1$, there exists a finite group G with elements a and b s.t. a has order m, b has order n, and ab has order r*

Proof. We shall show that, for a suitable prime power q, there exist elements a and b of $\mathrm{SL}_2(\mathbb{F}_q)$ s.t. a, b and ab have orders $2m, 2n$ and $2r$ respectively. As $-I$ is the unique element of order 2 in $\mathrm{SL}_2(\mathbb{F}_q)$, the image of a, b, ab in $\mathrm{SL}_2(\mathbb{F}_q)/\{\pm I\}$ will then have orders m, n and r as required.

Let p be the prime number not dividing $2mnr$. Then p is a unit in the finite ring $\mathbb{Z}/2mnr\mathbb{Z}$, and so some power of it, q say, is 1 in the ring. This means that $2mnr$ divides $q-1$. As the group $\mathbb{F}_q^\times$ has order $q-1$ and is cyclic (1.3), there exist element $u, v, w \in \mathbb{F}_q^\times$ having orders $2m, 2n$ and $2r$ respectively. Let

$$a = \begin{pmatrix} u & 1 \\ 0 & u^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q) \quad b = \begin{pmatrix} v & 0 \\ t & v^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$$

where t has been chosen so that

$$uv + t + u^{-1}v^{-1} = w + w^{-1}$$

The characteristic polynomial of a is $(X-u)(X-u^{-1})$ □

1.7 Exercises

Exercise 1.7.1. Let $n = n_1 + \cdots + n_r$ be a partition of the positive integer n. Use Lagrange's theorem to show that $n!$ is divisible by $\prod_{i=1}^{r} n_i!$

Proof. $n_1, \ldots, n_r$ is a partition of n elements, and S_{n_i} is the permutation group of each part.

Apparently each S_{n_i} is normal. Thus $S_{n_1} \ldots S_{n_r}$ is a subgroup of S. Also $S_{n_i} \cap S_{n_j} = \{\mathrm{id}\}$. Therefore $S_{n_1} \ldots S_{n_r} \cong S_{n_1} \times \cdots \times S_{n_r}$ ☐

Exercise 1.7.2. Let $N \lhd G$ of index n. Show that $g \in G \Rightarrow g^n \in N$

Proof. Because the group G/N has order n, $(gN)^n = 1$ for every $g \in G$. ☐

2 Free Groups and Presentations; Coxeter Groups

2.1 Free monoids

Let $X = \{a, b, c, \ldots\}$. A **word** is a finite sequence of symbols from X. Empty sequence is denoted by 1. Write SX for the set of words together with the binary concatenation. Then SX is a monoid, called the **free monoid** on X

$X \to SX$ has the following universal property: for any map of sets $\alpha : X \to S$ from X to a monoid S, there exists a unique homomorhism $SX \to S$ making the diagram

$$\begin{tikzcd} X \arrow[r, "a \mapsto a"] \arrow[dr, "\alpha"'] & SX \arrow[d, dashed] \\ & S \end{tikzcd}$$

commute

2.2 Free groups

We want to construct a group FX contianing X and having the same universal property. Define

$$X' = \{a, a^{-1}, b, b^{-1}, \ldots\}$$

Let W' be the set of words using symbols from X'. A word is **reduced** if it contains no pairs of the form aa^{-1} or $a^{-1}a$. Starting with a word w, we can perform a finite sequence of cancellations to arrive at a reduced word, which will be called the **reduced form** w_0 of w.

Proposition 2.1. *There is only one reduced form of a word*

Proof. Induction on the length of the word w. If w is reduced, there is nothing to prove. Otherwise a pair of the form $a_0 a_0^{-1}$ or $a_0^{-1} a_0$ occurs - assume the first

Observe that any two reduced forms of w obtained by a sequence of cancellations in which $a_0 a_0^{-1}$ is cancelled first are equal, because the induction hypothesis can be applied to the shorter word.

Next observed that any reduced forms of w obtained by a sequence of cancellations where $a_0 a_0^{-1}$ is cancelled at some point are equal, because the result of such a sequence of cancellations will not be affected if $a_0 a_0^{-1}$ is cancelled first

finally consider a reduced form w_0 obtained by a sequence where no cancellation cancels $a_0 a_0^{-1}$ directly. Since $a_0 a_0^{-1}$ doesn't remain in w_0, at least one of a_0 or a_0^{-1} is cancelled. But the word obtained after this cancellation is the same as if our original pair were cancelled $\square$

w, w' are **equivalent**, denoted $w \sim w'$, if they have the same reduced form

Proposition 2.2. *products of equivalent words are equivalent, i.e.,*

$$w \sim w', v \sim v' \Rightarrow wv \sim w'v'$$

Let FX be the set of equivalence classes of words. Proposition 2.2 shows that the binary operation on W' defines a binary operation on FX, which obviously makes it into a monoid. It also has inverses. Thus FX is a group, called the **free group**

Proposition 2.3. *For any map of sets $\alpha : X \to G$ from X to a group G, there exists a unique homomorhism $FX \to G$ making the following diagram commute*

$$\begin{tikzcd} X \arrow[r, "a \mapsto a"] \arrow[dr, "\alpha"'] & FX \arrow[d, dashed] \\ & G \end{tikzcd}$$

Proof. Consider a map $\alpha : X \to G$, and extend it to $X' \to G$ letting $\alpha(a^{-1}) = \alpha(a)^{-1}$. Because G is a monoid, α extends to a homomorhism of monoids $SX' \to G$. This map will send equivalent words to the same element of G, and so will factor through $FX = SX'/\sim$. $\square$

Corollary 2.4. *Every group is a quotient of a free group*

Proof. Choose a set X of generators for G (e.g. $X = G$), and let F be the free group generated by X. According to 2.3 the map $a \mapsto a : X \to G$ extends to a homomorhism $F \to G$, and the image, being a subgroup containing X, must equal G $\square$

Theorem 2.5 (Nielsen-Schreier)**.** *Subgroups of free groups are free*

Two free groups FX and FY are isomorphic iff $|X| = |Y|$. Thus **rank** of a free group G to be the cardinality of any free generating set (subset X of G for which the homomorhism $FX \to G$ given by 2.3 is an isomorphism)

2.3 Generators and relations

Consider a set X and a set R of words made up of symbols in X'. Each element of R represents an element of the free group FX, and the quotient G of FX by the normal subgroup generated by these elements is said to have X as **generators** and R as **relations**. (X, R) is a **presentation** for G, and denotes G by $\langle X \mid R \rangle$

Proposition 2.6. $G = \langle X \mid R \rangle$*, for any group H and map $\alpha : X \to H$ sending each element of R to 1, there exists a unique homomorhism $G \to H$ making the diagram commute*

$$\begin{tikzcd}
X \arrow[r, "a \mapsto a"] \arrow[dr, "\alpha"'] & G \arrow[d, dashed] \\
 & H
\end{tikzcd}$$

Proof.

$$\begin{tikzcd}
X \arrow[r, "\iota"] \arrow[dr] & FX \arrow[r] \arrow[d, dashed] & FX/(\iota R) = G \arrow[dl, dashed] \\
 & H &
\end{tikzcd}$$

$\square$

2.4 Finitely presented groups

A group is **finitely presented** if it admits a presentation (X, R) with both X and R finite

Example 2.1. Consider a finite group G. Let $X = G$, and let R be the set of words

$$\{abc^{-1} \mid ab = c\}$$

(X, R) is a presentation of G, and so G is finitely presented: let $G' = \langle X \mid R\rangle$. The extension of $a \mapsto a : X \to G$ to FX sends each element of R to 1, and therefore defines a homomorhism $G' \to G$, which is obviously surjective. But every element of G' is represented by an element of X, and so $|G'| \leq |G|$. Therefore the homomorhism is bijective

2.5 Coxeter groups

A **Coxeter system** is a pair (G, S) consisting of a group G and a set of generators S for G subject only to relations of the form $(st)^{m(s,t)} = 1$

$$\begin{cases} m(s,s) = 1 \text{ for all } s \\ m(s,t) \geq 2 \\ m(s,t) = m(t,s) \end{cases} \tag{1}$$

When no relation occurs between s and t, we set $m(s,t) = \infty$. Thus a Coxeter system is defined by a set S and a mapping

$$m : S \times S \to \mathbb{N} \cup \{\infty\}$$

satisfying (1), and the group $G = \langle S \mid R\rangle$ where

$$R = \{(st)^{m(s,t)} \mid m(s,t) \neq \infty\}$$

The **Coxeter groups** are those that arise as part of a Coxeter system. The cardinality of S is called the **rank** of the Coxeter system

2.6 Exercises

Exercise 2.6.1. Let $D_n = \langle a, b \mid a^n, b^2, abab\rangle$ be the nth dihedral group. If n is odd, prove that $D_{2n} \approx \langle a^n\rangle \times \langle a^2, b\rangle$, and hence that $D_{2n} \approx C_2 \times D_n$

Proof. first, $ab(b^{-1}a^{-1}) = ab(b^{-1}a^{-1})(abab) = abab = e$, hence D_n is commutative for any n. Since n is odd, $(n, 2) = 1$ and so $D_{2n} \approx C_2 \times C_n$ $\square$

3 TODO skip and problems

1.6 2.5