Compact course notes

Pure Math 346, Winter 2011

Group Theory

Professor: W.Kuo
transcribed by: J. Lazovskis
University of Waterloo
September 1, 2011

Contents

1 Types of groups

1.1 Base definitions

Definition 1.1.1. A binary operation on a set S is a function $S \times S \to S$. Define the binary operation as $*$ so we have $(a, b) \to a * b \in S$.

Definition 1.1.2. A group $G = (S, *)$ is a set S along with a binary operation $*$ satisfying

1. Associativity: for all $a, b \in S$, $a * (b * c) = (a * b) * c$
2. Identity: for all $a \in S$ there exists $e \in S$ such that $a * e = e * a = a$
   for every $a \in S$ there exists $b \in S$ such that $a * b = b * a = e$

Definition 1.1.3. If $*$ is commutative, that is, for all $a, b \in S$, $a * b = b * a$, then $G = (S, *)$ is termed an abelian group.

Definition 1.1.4. The size of a group G is given by $|G|$. It is also termed the order of the group. It describes the number of elements in the group.

Example 1.1.5. These are some of the more common groups:

$$
\begin{aligned}
(\mathbb{Z}, +) &= C_\infty \\
(\mathbb{Z}_n, +) &= (\mathbb{Z}/n\mathbb{Z}, +) \\
&= C_n \\
(\mathbb{Z}/n\mathbb{Z})^* &= U_n \\
&= (\{[a] \in \mathbb{Z}_n \,\big|\, (a, n) = 1\}, \cdot) \\
(S_n, *) &= (\text{the set of bijections on } \{1, \ldots, n\},\ \text{composition}) \\
&= (\text{the set of permutations on } \{1, \ldots, n\}, *) \\
D_n &= (\text{rotations and reflections of an } n\text{-gon}, *)
\end{aligned}
$$

1.2 Properties of groups

Proposition 1.2.1. The groups satisfy the cancellation law, i.e. for any $a, b, c \in G$, $ab = ac \implies b = c$.

Corollary 1.2.2. The identity element and inverses are unique.

Proposition 1.2.3. Let G be a group. Then

1. for all $a \in G$, $(a^{-1})^{-1} = a$
2. for all $n \in \mathbb{N}$, $(a^{-1})^n = (a^n)^{-1}$

Corollary 1.2.4. $(ab)^{-1} = b^{-1}a^{-1}$

Definition 1.2.5. Let G be a group. Then G is a finite group if $|G| < \infty$. Otherwise, G is an infinite group.

Proposition 1.2.6. If G is a finite group of even order, then G has an element of order 2.

Example 1.2.7. These are orders for some of the more common groups:

$|C_\infty| = |(\mathbb{Z}, +)| = \infty$ $\qquad$ $|U_n| = \varphi(n)$
$|C_n| = |(\mathbb{Z}/n\mathbb{Z})| = n$ $\qquad$ $|D_n| = 2n$
$|S_n| = n!$

Remark 1.2.8. The dihedral group may be defined as $D_n = \{a^i b^j \,\big|\, a^2 = b^n = 1, aba^{-1} = b^{-1}, i, j \in \mathbb{Z}\}$.

Definition 1.2.9. A group G is termed cyclic if there exists $g \in G$ such that for every $a \in G$, there exists $n \in \mathbb{Z}$ such that $g^n = a$. Such a g is termed a generator.

Corollary 1.2.10. Generators need not be unique.

Theorem 1.2.11. A cyclic group is an abelian group.

1.3 Subgroups

Definition 1.3.1. Let G be a group with $g \in G$. Define a subset $\langle g \rangle$ of G by $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} \subseteq G$. It is clear that $\langle g \rangle$ is a group under the binary operator of G.

· Identity: $g^0 = 1$

· Inverse: $(g^n)^{-1} = g^{-n}$

Then $\langle g \rangle$ is a group, and it is said to be generated by g.

Definition 1.3.2. If G is a group, a subset H is termed a <u>subgroup</u> of G if it is a group under the same binary operation of G. That is, H is a group if

1. for all $a, b \in H$, $ab \in H$

2. $1 \in H$

3. if $a \in H$, then $a^{-1} \in H$

Then this relationship is denoted $H \leqslant G$.

Definition 1.3.3. Let G be a group and $g \in G$. The <u>order</u> of g, denoted by $o(g)$, is the smallest positive integer n such that $g^n = 1$. If such an integer does not exist, g is said to have infinite order.

Theorem 1.3.4. Let G be a group and $g \in G$. Then $o(g) = |\langle g \rangle|$.

Theorem 1.3.5.∗ [Subgroup test]

Let G be a group and H a non-empty subset of G. Then

1. H is a subgroup of $G \iff$ for all $a, b \in H$, $ab^{-1} \in H$

2. If H is finite, H is a subgroup $\iff$ for all $a, b \in H$, $ab \in H$

Proposition 1.3.6.∗ Let G be a group and let $a, b \in G$ of finite order. Then

1. If $k \in \mathbb{N}$ and $a^k = 1$, then $o(a) \mid k$

2. If $k \in \mathbb{N}$, then $o(a^k) = \dfrac{o(a)}{\gcd(o(a), k)}$

3. If $\gcd(o(a), o(b)) = 1$ and $ab = ba$, then $o(ab) = o(a)o(b)$

Theorem 1.3.7.∗ A subgroup of a cyclic group is always cyclic.

Theorem 1.3.8.∗ A finite cyclic group of order n has precisely one subgroup of order m for each $m \in \mathbb{N}$ such that $m \mid n$. These are the only subgroups of the given group.

Definition 1.3.9. For a finite group G, define the <u>exponent</u> of G to be the smallest positive integer t such that $g^t = 1$ for all $g \in G$.

Note that the exponent of S_n is $\mathrm{lcm}(1, 2, \ldots, n)$.

Definition 1.3.10. For G a group and $g \in G$, define the <u>centralizer</u> of g in G to be the set

$$C(g) = \{x \in G \mid gx = xg\} \leqslant G$$

Note that $\langle g \rangle \subseteq C(g)$ for all $g \in G$.

Definition 1.3.11. For G a group, define the <u>center</u> of G to be the set

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\} \lhd G$$

1.4 Cosets

Definition 1.4.1. In general, for any group G and H a subgroup of that group with $a, b \in G$, we say that $a \equiv b \pmod{H} \iff a \equiv_H b \iff ab^{-1} \in H$.

Theorem 1.4.2. Let G be a group and H a subgroup of G. Then $a \equiv_H b$ is an equivalence relation.

Remark 1.4.3. Recall that for $G = C_\infty = (\mathbb{Z}, +)$ and $H = (n\mathbb{Z}, +)$, the equivalence relation $\equiv_H$, or multiplication modulo n, breaks $\mathbb{Z}$ into disjoint pieces, namely $\{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

Similarly, for G any group with $H \leqslant G$, the equivalence relation $\equiv_H$ breaks up G into a partition of pieces P for $P = \{a \mid a \equiv_H b, b \in P\}$. If we let $a \in G$ and Pa be the piece that contains a, then $b \in Pa \iff b \in Ha$, so $Pa = Ha$.

Further, there exists a bijection $\varphi : H \to Ha$ given by $h \mapsto ha$.

Definition 1.4.4. For G a group and $H \leqslant G$, the right coset of H is defined to be $Ha = \{ha \mid h \in H\} \subseteq G$ for fixed $a \in G$.

Remark 1.4.5. Since $\equiv_H$ is an equivalence relation, G can be expressed as a disjoint union of right cosets, or $G = \bigsqcup_{a_i \in R} Ha_i$ where R is a subset of G and for all $a_i, a_j \in R$, $a_i \neq a_j \implies a_i \not\equiv_H a_j$.

The same may be done with left cosets.

Definition 1.4.6. A set R with the properties described above is termed a set of representatives of cosets.

Remark 1.4.7. The sets of representatives of cosets are not unique.

· ${}^{G}\!/_{H}$ denotes the set of left cosets · ${}_{H}\backslash^{G}$ denotes the set of right cosets

Theorem 1.4.8. For G a group and $H \leqslant G$, there exists $R \subseteq G$ such that $G = \bigsqcup_{a_i \in R} Ha_i = \bigsqcup_{a_i \in R} a_i H$

Theorem 1.4.9.∗ [Lagrange]

If G is a group and H a subgroup of G, then $|H| \,\Big|\, |G|$. We denote $[G : H] = |G|/|H|$ to be the index of H.

Moreover, the index denotes the number of left cosets of H in G.

Corollary 1.4.10. Let G be a group and $g \in G$. then $o(g) \mid |G|$.

Corollary 1.4.11. Let G be a group with $|G| = p$ for p prime. Then G is cyclic.

Remark 1.4.12. In general, left cosets are different from right cosets.

Example 1.4.13. Consider $G = S_3 = \{1, a, a^2, b, ab, a^2b\}$ with $a^3 = 1$, $b^2 = 1$, and $ba = a^2b$.
Here, there are two nontrivial subgroups: $H_1 = \{1, a, a^2\}$ and $H_2 = \{1, b\}$.

Note that $H_1a^2 \neq a^2H_2$ and $H_1b \neq bH_2$.

Definition 1.4.14. Let G be group with $a \in G$. The map $b \mapsto aba^{-1} = c(a)b$ is termed the conjugation by a, denoted $c(a)$.

Thus for any $a \in G$, we have $c(a)H \subseteq H$.

1.5 Normal subgroups

Definition 1.5.1. A normal subgroup H of a group G is a subgroup such that $\forall a \in G$, $\forall h \in H$, $aha^{-1} \in H$. This relationship is denoted by $H \lhd G$.

Theorem 1.5.2. Let H be a subgroup of a group G. Then the following are equivalent:

1. H is normal
2. For all $g \in G$, $gH = Hg$.
3. Every right coset is a left coset.
4. Every left coset is a right coset.
5. For all $a, b \in G$, $ab \in H \implies ba \in H$.

Proposition 1.5.3. Let G be a group and p the smallest prime dividing $|G|$. If $H \leqslant G$ and $[G : H] = p$, then $H \lhd G$.

Definition 1.5.4. Let H, K be two subsets of a group G. Then $HK = \{hk \,\big|\, h \in H, k \in K\}$.

Remark 1.5.5. Let H be a subgroup of a group G. Then for $a, b \in G$, $HaHb = Hab$.

Theorem 1.5.6. Let G be a group and N be a normal subgroup of G. Let ${}^{G}\!/_{N}$ be the set of cosets. Define for all $a, b \in G$, $Na * Nb = Nab$. Then $\left({}^{G}\!/_{N}, *\right)$ is a group.

Definition 1.5.7. The above described group $\left({}^{G}\!/_{N}, *\right)$ is termed the quotient group of G modulo N.

Remark 1.5.8. Note that for any group G, $Z(G) \lhd G$ and $|{}^{G}\!/_{Z(G)}|$ is never prime.

Theorem 1.5.9. Let G be a group with $N, H \leqslant G$. Then
1. $N \lhd G \Longrightarrow HN \leqslant G$
2. $N, H \lhd G \Longrightarrow HN \lhd G$
3. $N \cap H \leqslant G$
4. $N \lhd G \Longrightarrow N \cap H \lhd H$
5. $N, H \lhd G \Longrightarrow N \cap H \lhd G$

2 Morphisms

2.1 Types of morphisms

Definition 2.1.1. A homomorphism f from a group G to a group H is a function $f : G \to H$ satisfying $f(a *_G b) = f(a) *_H f(b)$.

Remark 2.1.2. With respect to the above definition, it may be easily shown from that $1_H = f(1_G)$ and $f(a^{-1}) = f(a)^{-1}$.

Definition 2.1.3. An isomorphism is a bijective homomorphism. An automorphism is an isomorphism from a group to itself.

Remark 2.1.4. Given two groups G, H, there is a homomorphism $1 : G \to H$ given by $g \mapsto 1_H$ for all $g \in G$. This is termed the trivial homomorphism.

Similarly, the map $\mathrm{id} : G \to G$ given by $g \mapsto g$ is an automorphism termed the identity map.

Proposition 2.1.5. Let $f : G \to H$ and $g : H \to K$ be homomorphisms. Then
1. $g \circ f : G \to K$ is a homomorphism
2. If $f : G \to H$ is an isomorphism, then $f^{-1} : H \to G$ is also an isomorphism.

Remark 2.1.6. If groups G and H are isomorphic, then there exists an isomorphism between them. This equivalence relation is denoted $G \cong H$. They also share the same group structure (in terms of subgroups).

Theorem 2.1.7. Any two cyclic groups of the same order are isomorphic.

Definition 2.1.8. Suppose that $\varphi : G \to H$ is a homomorphism.
1. Define the image of φ to be $\mathrm{Im}(\varphi) = \{h \in H \,\big|\, \text{there exists } g \in G \text{ such that } h = \varphi(g)\}$
2. Define the kernel of φ to be $\ker(\varphi) = \{g \in G \,\big|\, \varphi(g) = 1_H\}$

Theorem 2.1.9. Let G be a group and $N \leqslant G$. Then $N \lhd G \iff N = \ker(\varphi)$ for some homomorphism φ.

Remark 2.1.10. The symmetric group S_3 has the following properties:
1. The smallest non-abelian group is S_3
2. Any non-abelian group of order 6 is isomorphic to S_3
3. The elements of S_3 can be represented as $\{1, a, a^2, b, ab, a^2b\}$ where $a^3 = 1$, $b^2 = 1$, and $ba = a^2b$

2.2 Morphism theorems

Theorem 2.2.1. Let $\varphi : G \to H$ be a homomorphism for groups G, H. Then

1. $\operatorname{Im}(\varphi) \leqslant H$
2. $\ker(\varphi) \lhd G$
3. φ is injective $\iff$ $\ker(\varphi) = \{1_G\}$

Theorem 2.2.2. Let G, H be finite groups with $\varphi : G \to H$ a homomorphism. Then $o(\varphi(g)) \,\big|\, o(g) \;\; \forall \;\; g \in G$.

Remark 2.2.3. If a function between finite sets is injective (one-to-one), then it is also surjective (onto).

Proposition 2.2.4. If $f : A \to B$ is a bijection for sets A, B, then there exists $e \in A$ such that $f(e) = e$.

Definition 2.2.5. Let G, H be groups. Then the direct product of G and H is a group, denoted by $(G \times H, *)$.
· $G \times H = \{(g, h) \,\big|\, g \in G, h \in H\}$ with $(g, h) * (g', h') = (gg', hh')$ for all $g, g' \in G$ and $h, h' \in H$

Definition 2.2.6. Given a group G, a group H is termed a homomorphic image of G if there exists a homomorphism from G to H.

Remark 2.2.7. Let $N \lhd G$ for a group G. Then ${}^{G}\!/_{N}$ is a homomorphic image of G described by the homomorphism $\varphi : G \to {}^{G}\!/_{N}$ defined by $g \mapsto gN$.

Theorem 2.2.8. [1st isomorphism theorem]
Let $\varphi : G \to H$ be an isomorphism for groups G, H. Then $\operatorname{Im}(\varphi) \cong {}^{G}\!/_{\ker(\varphi)}$.

Theorem 2.2.9. [2nd isomorphism (or correspondence) theorem]
For G a group with $N \lhd G$, every subgroup of ${}^{G}\!/_{N}$ is of the form ${}^{H}\!/_{N}$ with $H \leqslant G$ and $N \subseteq H$.

Theorem 2.2.10. [3rd isomorphism theorem]
Suppose that G is a group with $N \lhd G$. Then

1. ${}^{H}\!/_{N} \lhd {}^{G}\!/_{N} \iff H \lhd G$
2. ${}^{H}\!/_{N} \lhd {}^{G}\!/_{N} \Longrightarrow \dfrac{{}^{G}\!/_{N}}{{}^{H}\!/_{N}} \cong {}^{G}\!/_{H}$

2.3 Products of subgroups

Definition 2.3.1. Let G be a group and $H, K \leqslant G$. Then $HK = \{hk \,\big|\, h \in H, k \in K\}$.

Proposition 2.3.2.$*$ Suppose G is a finite group with $H, K \leqslant G$. Then $|HK| = \dfrac{|H||K|}{|H \cap K|} = |KH|$

Remark 2.3.3. If for a group G, we have $H, K \leqslant G$, then also $H \cap K \leqslant G$.

Remark 2.3.4. Let G be a group with $H, K \leqslant G$. If $H \cap K = \{1\}$ and $|H||K| = |G|$, then $HK = G$.

Proposition 2.3.5. Let G be a group with $H, K \leqslant G$. Then the following are equivalent:

1. $HK \leqslant G$
2. $KH \leqslant G$
3. $KH = HK$

Lemma 2.3.6. Let G be a group with $L, M \lhd G$. If $L \cap M = \{1\}$, then for all $\ell \in L$ and $m \in M$, $\ell m = m\ell$.

Theorem 2.3.7. [Internal characterization of the direct product]
Let G, H, K be groups. Then $G \cong H \times K$ if and only if there exist $H^* \lhd G$ and $K^* \lhd G$ such that

1. $H \cong H^*$ and $K \cong K^*$
2. $H^* \cap K^* = \{1_G\}$
3. $H^* K^* = G$

Lemma 2.3.8. Let G be a group and $a, b \in G$ with prime orders. Then either $\langle a \rangle = \langle b \rangle$ or $\langle a \rangle \cap \langle b \rangle = \{1_G\}$.

3 The permutation group S_n

3.1 Construction

Definition 3.1.1. Elements $\alpha, \beta \in S_n$ are termed disjoint if $\alpha(i) \neq i \Longrightarrow \beta(i) = i$ for all $i \in \{1, \ldots, n\}$.

Remark 3.1.2. The above is a symmetric statement: $\left[\alpha(i) \neq i \Longrightarrow \beta(i) = i\right] \iff \left[\alpha(i) = i \Longrightarrow \beta(i) \neq i\right]$

Theorem 3.1.3. If α, β are disjoint, then $\alpha\beta = \beta\alpha$.

Theorem 3.1.4. If α, β are disjoint, then $o(\alpha\beta) = \operatorname{lcm}(o(\alpha), o(\beta))$.

Definition 3.1.5. Given $\alpha \in S_n$, define an equivalence relation $\sim_\alpha$ on $\{1, \ldots, n\}$ by $i \sim_\alpha j \iff$ there exists $\ell \in \mathbb{Z}$ such that $\alpha^\ell(i) = j$.

Then $\sim_\alpha$ breaks $\{1, \ldots, n\}$ into partitions: $\{1, \ldots, n\} = \displaystyle\bigsqcup_{t=1}^{m} C_t$ where $C_p \cap C_\ell = \emptyset \iff p \neq \ell$.

Definition 3.1.6. Let $\alpha \in S_n$. Then the cycle structure of α is $\left[|C_1|, |C_2|, \ldots, |C_m|\right]$.

Remark 3.1.7. The cycle structure $[n_1, \ldots, n_m]$ has the property that $\displaystyle\sum_{t=1}^{m} n_t = n$ and $n_\ell \geqslant n_p \iff \ell \geqslant p$.

Definition 3.1.8. The cycle notation of a group G is $\alpha = (a_1\ a_2\ \ldots\ a_k)(b_1\ b_2\ \ldots\ b_\ell)\cdots$ if $\alpha(a_i) = a_{i+1}$ and $\beta(b_j) = b_{j+1}$ for $1 \leqslant i \leqslant k-1$ and $1 \leqslant j \leqslant \ell - 1$ and $\alpha(a_k) = a_1$ and $\beta(b_\ell) = b_1$. For simplicity, singletons are omitted.

It should be noted that cycle notation is not unique.

Theorem 3.1.9. Every permutation α may be expressed as a product of disjoint cycles $\alpha_1\alpha_2\ldots\alpha_m$ where $\alpha_i = \begin{cases} \alpha_t(i) & i \in C_t \\ i & i \notin C_t \end{cases}$ where all the C_j's come from $\sim_\alpha$.

Further, we have that $\alpha = \alpha_1\alpha_2\cdots\alpha_m$ and α_t is a $|C_t|$-cycle.

Also note that α^{-1} has the same cycle structure as α.

Theorem 3.1.10. The number of elements N_p in S_n with the cycle structure $[n_1, \ldots, n_m] = p$ is given by

$$N_p = \frac{n!}{\displaystyle\prod_{t=1}^{n} t^{\ell_t}\ell_t!} \qquad \text{where } 1 \leqslant \ell_t \leqslant n \text{ is the number of } n_i\text{'s equal to } t$$

Example 3.1.11. Let $\alpha = (1\ 2\ 5)(3\ 7)(4\ 8)(9\ 6)(10)$. Then $N_p = \frac{10!}{(3^1\cdot 1!)(2^3\cdot 3!)(1^1\cdot 1!)}$.

Theorem 3.1.12. If $\alpha \in S_n$ has the cycle structure $[n_1, \ldots, n_m]$, then $o(\alpha) = \operatorname{lcm}(n_1, \ldots, n_m)$.

Theorem 3.1.13. Suppose that $\alpha \in S_n$ has m_j j-cycles for each $j \in \{1, 2, \ldots, n\}$. Then

$$|C(\alpha)| = \prod_{j=1}^{n} j^{m_j} m_j!$$

3.2 The alternating group

Definition 3.2.1. Any element with the cycle structure $[2, 1, 1, \ldots, 1]$ is termed a transposition.

Definition 3.2.2. Let G be a group. Let S be a subset of G. The subgroup $\langle S\rangle$ generated by S is the subset of G defined as:

$$\langle S\rangle = \{s_1^{\ell_1}s_2^{\ell_2}\ldots s_k^{\ell_k} \mid s_i \in S, \ell_i \in \mathbb{Z}, k \in \mathbb{N}\cup\{0\}\}$$

Remark 3.2.3. Let S be the set of all transpositions. Then S_n is generated by S.

Definition 3.2.4. Let $\alpha \in S_n$. Then

1. α is <u>even</u> if it can be expressed as an even number of transpositions

2. α is <u>odd</u> if it can be expressed as an odd number of transpositions

Lemma 3.2.5. Suppose $\alpha \in S_n$ is a product of k transpositions. Then exactly one of the following hold for all $a \in \{1, 2, \ldots, n\}$:

1. $\alpha(a) \neq a$

2. α may be expressed as a product of $k-2$ transpositions

Definition 3.2.6. Let $\varphi : S_n \to C_2$ given by $\alpha \mapsto \begin{cases} [0] & \alpha \text{ even} \\ [1] & \alpha \text{ odd} \end{cases}$ Then φ is a surjective homomorphism. Further, define $A_n = \ker(\varphi)$ to be the <u>alternating group</u>.

Remark 3.2.7. Conjugation preserves cycle structure.

That is, if $\alpha = (1\ \ 3\ \ 5)(4\ \ 2)$, then $c(\beta)\alpha = \beta\alpha\beta^{-1} = (\beta(1)\ \ \beta(3)\ \ \beta(5))(\beta(4)\ \ \beta(2))$

Theorem 3.2.8. Two permutation groups in S_n are conjugate $\iff$ they have the same cycle structure.

Corollary 3.2.9. The number of conjugacy classes of S_n is the same as the number of cycle structures is the same as the number of partitions of n.

Definition 3.2.10. A group G is termed <u>simple</u> if it has exactly two normal subgroups, $\{1_G\}$ and G.

Proposition 3.2.11. For $n \geqslant 3$, A_n is generated by 3-cycles. Moreover, the only subgroup of S_n generated by 3-cycles is A_n.

Note that an m-cycle is odd (even) if m is even (odd).

Lemma 3.2.12. If $\alpha \in S_n$ has cycle structure $[n_1, \ldots, n_m]$, then α is even (odd) $\iff$ $n+m$ is even (odd).

Theorem 3.2.13. If the following hold:

· $n \geqslant 4$

· $N \lhd A_n$ with $N \neq \{1\}$

· N contains a 3-cycle

then $N = A_n$.

Proposition 3.2.14. A_4 has no subgroup of order 6.

Theorem 3.2.15. [Burnside theorem]

Any non-cyclic group of odd order is not simple.

Theorem 3.2.16. If $n \geqslant 5$, then A_n is simple.

Theorem 3.2.17. The only subgroup of S_n of order $\frac{n!}{2}$ is A_n.

Remark 3.2.18. For p an odd prime, A_p has a subgroup of order $2p$ if and only if $p \equiv 1 \pmod 4$.

4 Group actions

4.1 Mappings

Definition 4.1.1. An <u>action of a group</u> G (a group action) on a set X is a function $\varphi : G \times X \to X$ given by $(g, x) \mapsto \varphi(g, x)$ satisfying:

i. $\varphi(gh, x) = \varphi(g, \varphi(h, x))$ for all $g, h \in G$, $x \in X$

ii. $\varphi(1, x) = x$ for all $x \in X$

To simplify notation, we write $\varphi_g(x) = \bar{g} := \varphi(g, x)$ for $\varphi_g : X \to X$.

Also note that since $\varphi_g \circ \varphi_{g^{-1}} = \varphi_{gg^{-1}} = \varphi_1 = 1$, φ_g is a bijection.

Remark 4.1.2. Let S_X be the set of all permutations on the set X, i.e. all bijections between X and itself. Then S_X is a group and $\psi : G \to S_X$ given by $g \mapsto \varphi_g$ is a group homomorphism.

Thus, a group action is simply a homomorphism from G to S_X.

Conversely, if $\psi : G \to S_X$ is a group homomorphism, then define $\varphi : G \times X \to X$ by $\varphi(g, x) \mapsto \psi(g)(x)$. Then φ is a group action.

Definition 4.1.3. Suppose that $\varphi : G \times X \to X$ is a group action on the set X. Define an equivalence relation on X by $x \sim_\varphi y \iff$ there exists $g \in G$ such that $\varphi(g, x) = y$ or $\varphi_g(x) = y$.

Definition 4.1.4. Let $x \in X$. Define

i. the <u>stabilizer</u> by $S_G(x) := \{g \in G \,|\, \bar{g}(x) = x\} \leqslant G$

ii. the <u>orbit</u> of x by $\mathcal{O}(x) := \{y \in X \,|\,$ there exists $g \in G$ such that $\bar{g}(x) = y\} \leqslant X$

Proposition 4.1.5. $\sim_\varphi$ is an equivalence relation (homomorphism).

Proposition 4.1.6. $S_G(x)$ is a subgroup of G for fixed x. Also, $|\mathcal{O}(x)| = \frac{|G|}{|S_G(x)|}$

4.2 Basic examples of group actions

Action 4.2.1.
G : a group
X : the group G
φ : given by $\varphi(g, x) = gx$
$S_G(x) = \{1\}$

Action 4.2.2.
G : a group
X : the set of left cosets of a subgroup H of G, or $\{gH \,|\, g \in G\}$
φ : given by $\varphi(g, aH) = gaH$
$S_G(aH) = \{aha^{-1} \,|\, h \in H\}$

Action 4.2.3.
G : a group
X : the group G
φ : given by $\varphi(g, x) = gxg^{-1}$
$S_G(x) = C_G(x)$

Action 4.2.4.
G : a group
X : the set $\{gHg^{-1} \,|\, g \in G\}$ for H a subgroup of G. This is the set of all conjugate subgroups of G.
φ : given by $\varphi(g, aHa^{-1}) = gaHa^{-1}g^{-1}$
$S_G(x) = N_G(H)$

Theorem 4.2.5. [Cayley]
A finite group of order n is isomorphic to a subgroup of S_n.

Theorem 4.2.6. Let G be a finite group with a proper subgroup H. If $|G| \nmid [G : H]!$, then G is not simple, so there exists a non-trivial normal subgroup of G.

4.3 Class equations

Definition 4.3.1. Consider the action of G on X where both G and X are finite. Then X is a disjoint union of orbits: $X = \bigsqcup_{\substack{\text{one } x \text{ from} \\ \text{each orbit}}} \mathcal{O}(x)$. This is termed the <u>class equation</u>.

Then we have $|X| = \sum_{\substack{\text{one } x \text{ from} \\ \text{each orbit}}} |\mathcal{O}(x)| = \sum_{\substack{\text{one } x \text{ from} \\ \text{each orbit}}} \frac{|G|}{|S_G(x)|}$. This is the <u>equivalence class equation</u>.

Definition 4.3.2. Let G be a group and X a set on which G acts. Then define $\mathrm{Fix}_G(X) := \{x \in X \,|\,$ for all $g \in G, \bar{g}(x) = x\}$. These are elements in X whose orbit has size 1.

Then the equivalence class equation can be rewritten as $|X| = |\mathrm{Fix}_G(X)| + \sum_{\substack{\text{one } x \text{ from} \\ \text{each orbit} \\ \text{with size}>1}} \frac{|G|}{|S_G(x)|}$

Equivalently, this may be expressed as $|G| = |Z(G)| + \sum_{\substack{\text{one } a \text{ from} \\ \text{each conjugacy} \\ \text{class with size}>1}} \frac{|G|}{|C_G(a)|}$

Remark 4.3.3. A group of order 15 is cyclic.

Proposition 4.3.4. Given $p_1, p_2, \dots, p_n$ distinct primes, $C_{p_1^{k_1}} \times C_{p_2^{k_2}} \times \cdots \times C_{p_n^{k_n}} \cong C_{p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}}$

4.4 Cauchy's theorem

Theorem 4.4.1. [Cauchy]
For G a finite group and p a prime divisor of $|G|$, there exists $g \in G$ with $o(g) = p$.

Definition 4.4.2. For p prime, G is a <u>p-group</u> if p is the only prime divisor of $|G|$, i.e. $|G| = p^k$, $k \in \mathbb{N}$.

Theorem 4.4.3. A non-trivial p-group G has a non-trivial center, i.e. $Z(G) \neq \{1\}$.

Corollary 4.4.4. If $|G| = p^2$ for p prime, then G is abelian.

Corollary 4.4.5. If $|G| = p^2$ for p prime, then $G \cong C_{p^2}$, or $G \cong C_p \times C_p$.

Theorem 4.4.6. If $|G| = pq$ for $p \leqslant q$ primes with $p \nmid (q-1)$, then G is abelian, i.e. $G \cong C_{pq}$ or $G \cong C_p \times C_q$.

Definition 4.4.7. The <u>quaternion group</u> Q is a group of order 8 with the following properties:
i. $Q = \langle a \rangle \langle b \rangle$ where $a^4 = b^4 = 1$, $a^2 = b^2$, and $aba^{-1} = b^3$
ii. $Q = \{i, j, k, 1, -i, -j, -k, -1\}$ with
$ij = k \quad ij = -ji$
$jk = i \quad jk = -kj$
$ki = j \quad ki = -ik$
$i^2 = j^2 = k^2 = -1$

Example 4.4.8. This is a realization of the quaternion group:

$$Q = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \pm \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \right\}$$

Theorem 4.4.9. If $|G| = 2p$ for p an odd prime, then either G is abelian, or G is the p-dihedral group. That is, either $G \cong C_{2p}$ or $G \cong D_p$.

5 Finite abelian group classification

5.1 Sylow's theorem

Definition 5.1.1. Let G be a finite group and p prime. A <u>Sylow p-subgroup</u> of G is a maximal p-subgroup of G. That is, if H is a Sylow p-subgroup of G, then
i. $|H| = p^k$ for some $k \in \mathbb{N}$ if $p^k \,\big|\, |G|$
ii. If $H \leqslant L \leqslant G$, and $|L| = p^m$ for some $m \in \mathbb{N}$, then $H = L$.

Definition 5.1.2. The <u>normalizer</u> of H in G is $N_G(H) = \{g \in G \,|\, ghg^{-1} \in H \ \forall \ h \in H\}$, where G is a group and $H \leqslant G$. This is also the stabilizer of H under conjugation, that is, $H \lhd N_G(H) \leqslant G$.
$N_G(H)$ is the largest subgroup K such that $H \lhd K$.

Lemma 5.1.3. Let G be a finite group and P a Sylow p-subgroup for p prime. If $g \in G$ satisfies
i. $o(g) = p^k$ for some $k \in \mathbb{Z}$
ii. $gPg^{-1} = P$, i.e. $g \in N_G(P)$
then $g \in P$.

Corollary 5.1.4. Let G be a finite group and P a Sylow p-subgroup. Then $p \nmid \left| {}^{N_G(P)}\!/_{P} \right|$.

Theorem 5.1.5. [Sylow]
Let G be a finite group and p prime. Suppose that $|G| = p^k m$ for some $k \in \mathbb{N}$ with $\gcd(p, m) = 1$. Then

1. Every Sylow p-subgroup of G has order p^k
2. The Sylow p-subgroups are all conjugate
3. The number of Sylow p-subgroups n_p satisfies
   - **i.** $n_p \equiv 1 \pmod p$
   - **ii.** $n_p \,\big|\, m$

Remark 5.1.6. Let P be a Sylow p-subgroup. Then for all $g \in G$, gPg^{-1} is also a Sylow p-subgroup.

Corollary 5.1.7. Let G be finite group and p prime. If $p^k \,\big|\, |G|$, then there exists $H \leqslant G$ with $|H| = p^k$.

Corollary 5.1.8. A Sylow p-subgroup is normal $\iff$ $n_p = 1$.

Remark 5.1.9. For p an odd prime, S_p has $(p-2)!$ Sylow p-subgroups.

5.2 Classification theory

Proposition 5.2.1. Let A be abelian with $a, b \in A$. Then

1. $o(a+b) \,\big|\, \operatorname{lcm}(o(a), o(b))$
2. If $\gcd(o(a), o(b)) = 1$, then $o(a+b) = o(a)o(b)$
3. $o(ka) = \dfrac{o(a)}{\gcd(o(a), k)}$

Definition 5.2.2. Let A be abelian. Then A is termed a <u>torsion group</u> if every element in A is of finite order. Similarly, A is termed <u>torsion-free</u> if every element of $A \setminus \{0\}$ is of infinite order. Note that $\{0\}$ is the only group that has both properties.

Definition 5.2.3. Define the <u>torsion part</u> of an abelian group A to be $T(A) = \{a \in A \,\big|\, o(a) < \infty\}$.

Theorem 5.2.4.∗ If A is abelian, then

1. $T(A) \leqslant A$
2. ${}^{A}\!/_{T(A)}$ is torsion-free

Theorem 5.2.5. [Primary decomposition]
Let A be a finite abelian group and $|A| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the prime decomposition of $|A|$. Let P_i be a Sylow p_i-subgroup of A. Then $A \cong P_1 \times \cdots \times P_k$.

In other words, a finite abelian group is isomorphic to the direct product of its Sylow subgroups.

Lemma 5.2.6. Let A be abelian and finite with at most $p-1$ elements of order p. Then A is cyclic.

Theorem 5.2.7. Let A be a finite abelian p-group and $a \in A$ with maximum order. Then

1. There exists a surjective homomorphism $\alpha : A \to \langle a \rangle$
2. $A \cong \ker(\alpha) \times \langle a \rangle$

Corollary 5.2.8. Any finite abelian group is a direct product of cyclic groups.

Remark 5.2.9. Let $A = C_{p^k}$. The number of elements of order at most p^n in A is $p^{\min(k,n)}$.

5.3 Structure theorems

Theorem 5.3.1. [Structure theorem for finite abelian groups]
A finite abelian group is isomorphic to a finite direct product of cyclic groups of prime power order. The decomposition is unique up to the order of the cycles. In other words,

$$|A| = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \Longrightarrow A \cong \prod_{i=1}^{k} \left(\prod_{j=1}^{m} C_{{p_i}^{\alpha_j}} \right) \qquad \text{with } \alpha_j \geqslant \alpha_{j-1} \;\; \forall \;\; j$$

Remark 5.3.2. If $|G| = p^k$ for G an abelian group, the number of possible groups G is the number of partitions of k.

Example 5.3.3. For $k = 4$, the 5 unique partitions are $4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$.

Definition 5.3.4. Let G be a group and $S \subseteq G$. Then G is said to be generated by S if G can be expressed as $G = \{a_1^{m_1}, a_2^{m_2}, \ldots, a_k^{m_k} \,|\, a_i \in S, m_i \in \mathbb{Z}\}$. The a_i's need not be unique.

Definition 5.3.5. If there exists a finite subset $S \subseteq G$ for G a group such that G is generated by S, then G is said to be finitely generated.

Remark 5.3.6. Let $G = (C_\infty)^k \cong \underbrace{C_\infty \times C_\infty \times \cdots \times C_\infty}_{k \text{ times}} \cong \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{k \text{ times}}$. Then G can not be generated by a subset S of size less that k.

Lemma 5.3.7. Let A be a non-trivial torsion-free abelian group. Suppose there exists $a \in A$ such that $\left| A/\langle a \rangle \right|$ is finite. Then $A \cong C_\infty$.

Theorem 5.3.8. Let A be finitely generated and of infinite order. Then

1. There exists a surjective homomorphism $\alpha : A \to C_\infty$

2. $A \cong \ker(\alpha) \times C_\infty$

Theorem 5.3.9. [Structure theorem for finitely generated abelian groups]
Let A be a finitely generated abelian group with ℓ generators. Then A is isomorphic to a finite direct product of cyclic groups, each with either infinite or prime power order. This decomposition is unique up to order.

Definition 5.3.10. Let A be a finitely generated abelian group and $A \cong T(A) \times (C_\infty)^k$. The number k is termed the rank of A.

Lemma 5.3.11. Let G be a group and $k \in G$. Then c_k is an automorphism on G.

Remark 5.3.12. For G a group and $N, K \leqslant G$, if

i. $NK = G$

ii. $N \cap K = \{1\}$

iii. $N \lhd G$

Then for all $k \in K$, c_k can act on N since N is normal. Thus there exists a mapping $\varphi : K \to \mathrm{Aut}(N)$ given by $k \mapsto c_k$ on N, with $n \mapsto knk^{-1}$.

Remark 5.3.13. For ease of notation, write $\varphi(k) = \varphi_k$ for $k \in K$.

Proposition 5.3.14. With respect to the above description, φ is an isomorphism.

Remark 5.3.15. $\mathrm{Aut}(G)$ is a group under the composition binary operation.

5.4 Semi-direct products

Definition 5.4.1. Let N, K be groups and $\varphi : K \to \mathrm{Aut}(N)$ a homomorphism. Define $N \rtimes K$, the semi-direct product of N by K, to be the set $N \times K = \{(n, k) \,|\, n \in N, k \in K\}$ with binary operation $*$ given by $(n_1, k_1) * (n_2, k_2) = (n_1 \varphi_{k_1}(n_2), k_1 k_2)$.

Theorem 5.4.2. Let N, K be groups with $\varphi : K \to \mathrm{Aut}(N)$. Then the semi-direct product $N \rtimes K = (N \times K, *)$ is a group, for φ and $*$ as above.

Theorem 5.4.3. [Internal characterization of the semi-direct product]
Let G, N, K be groups with $\varphi : K \to \mathrm{Aut}(N)$ a homomorphism. If $N^*, K^* \leqslant G$ with

i. $\alpha : N \cong N^*$, $\beta : K \cong K^*$ homomorphisms

ii. $N \lhd G$, $K \leqslant G$ and $\varphi^* : K^* \to \mathrm{Aut}(N^*)$ such that for all $n \in N, k \in K$, we have $\varphi^*(\beta(k))(n^*) = \varphi(k)$

iii. $N^* \cap K^* = \{1\}$

iv. $N^* K^* = G$

Then $G \cong N \rtimes K$.

Remark 5.4.4. The above may be represented in diagram form:

$$\begin{tikzcd}
K \arrow[r, "\beta"] \arrow[d, "\varphi"'] & K^* \arrow[d, "\varphi^*"] \\
\mathrm{Aut}(N) \arrow[r] & \mathrm{Aut}(N^*) \\
f \arrow[r, mapsto, "\tilde{\alpha}"] & \tilde{\alpha}(f(n^*)) = f(\alpha^{-1}(n^*))
\end{tikzcd}$$

This demonstrates commutativity, in that $\tilde{\alpha} \circ \varphi = \varphi^* \circ \beta$, for $\tilde{\alpha} : \mathrm{Aut}(N) \to \mathrm{Aut}(N^*)$.

Remark 5.4.5. Let G be a group with $N \lhd G$ and $K \leqslant G$ with $N \cap K = \{1\}$ and $NK = G$. Then to understand G, we only need to know the mapping $\varphi : K \to \mathrm{Aut}(N)$.

Definition 5.4.6. An inner automorphism is an automorphism induced by conjugation.

$$\begin{aligned}\mathrm{Inn}(N) &= \text{ the set of all inner automorphisms} \\ &= \{c_k \,\big|\, k \in N\}\end{aligned}$$

If N is abelian, then $\mathrm{Inn}(N) = \{\mathrm{Id}_N\}$.

Theorem 5.4.7. Let G be a group. Then

1. $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$

2. There exists a homomorphism $\alpha : G \to \mathrm{Inn}(G)$ given by $g \mapsto c_g$ for $g \in G$ with $\ker(\alpha) = Z(G)$. Thus $\mathrm{Inn}(G) \cong {}^{G}\!/_{Z(G)}$.

Remark 5.4.8. If $\varphi : K \to \mathrm{Aut}(N)$ is trivial, i.e. $\varphi_k = \mathrm{Id}_N$, then $(n_1, k_1) * (n_2, k_2) = (n\varphi_{k_1}(n_2), k_1k_2) = (n_1n_2, k_1k_2)$. That is, $N \rtimes K \cong N \times K$, and $\rtimes$ is just the direct product.

Remark 5.4.9. $\mathrm{Aut}(C_n) \cong U(n) = (\mathbb{Z}/n\mathbb{Z})^*$
That is, every $\varphi \in \mathrm{Aut}(C_n)$ can be associated with an integer in $U(n)$. Also, note that $\mathrm{Aut}(C_\infty) \cong C_2$.

Theorem 5.4.10. $U(p) \cong (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic for p prime.

Theorem 5.4.11. Given a group $G \cong C_m \rtimes C_n$,

$$G = \{x^i y^j \,\big|\, x^n = y^m = 1, x^{-1}yx = y^{-1}\}$$

Definition 5.4.12. Let p be prime and $n \in \mathbb{N}$. Then n is a primitive root if $[n]_p$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, i.e. $o([n]_p) = p - 1$.

Theorem 5.4.13. [Primitive Root theorem]
For any prime p there exists a primitive root.

Theorem 5.4.14. Let $|G| = pq$ with primes $p < q$ and $q \equiv 1 \pmod{p}$. Then there exists a unique (up to isomorphism) non-abelian group of order pq.

Remark 5.4.15. Let $N, K \leqslant G$ with $N \lhd G$ and $N \rtimes K \cong G$. Then $N \times K \cong G \iff$ any $\varphi : K \to \mathrm{Aut}(N)$ is trivial. In particular, if N, K are abelian, then G is abelian $\iff \varphi$ is trivial.

5.5 Solvability

Definition 5.5.1. For G a group, $c \in G$ is termed a commutator, denoted $c := [a, b]$, if there exist $a, b \in G$ such that $c = aba^{-1}b^{-1}$.

Proposition 5.5.2.

i. $[a, b] = 1 \iff ab = ba$

ii. $[a, b]^{-1} = [b, a]$

iii. For all $\varphi \in \mathrm{Aut}(G)$, $\varphi([a, b]) = [\varphi(a), \varphi(b)]$

iv. A product of 2 commutators is not necessarily a commutator.

Definition 5.5.3. For G a group, the commutator group G' of G is the subgroup of G generated by commutators of G.

Proposition 5.5.4. ${}^{G}/_{G'}$ is abelian.

Remark 5.5.5. If G is abelian, then $G' = \{1\}$.

Theorem 5.5.6. [Universal property of G']
For G a group and $\varphi : G \to A$ a homomorphism for A abelian, there exists a unique homomorphism $\beta : {}^{G}/_{G'} \to A$ such that the following diagram commutes:

$$\begin{tikzcd} G \arrow[rr, "\gamma"] \arrow[dr, "\alpha"'] & & {}^{G}/_{G'} \arrow[dl, "\beta"] \\ & A & \end{tikzcd}$$

Thus $\beta \circ \gamma = \alpha$.

Definition 5.5.7. For G a group, define the nth derived group as:

1. $G^{(1)} = G'$
2. $G^{(n+1)} = (G^{(n)})'$

Clearly, ${}^{G^{(n)}}/_{G^{(n+1)}}$ is abelian for all $n \in \mathbb{N}$.

Definition 5.5.8. A group G is termed solvable if there exists $n \in \mathbb{N}$ such that $G^{(n)} = \{1\}$ and $G^{(n-1)} \neq \{1\}$.

Remark 5.5.9.

i. If $H \leqslant G$, then $H' \leqslant G' \cap H$.
ii. If there exists a homomorphism $\alpha : G \to H$, then $\alpha(G') = H'$.

Theorem 5.5.10.

1. If G is solvable, then so is every subgroup and homomorphic image of G.
2. For G a group and $N \lhd G$, N and ${}^{G}/_{N}$ are solvable $\iff$ G is solvable.

6 Detailed classification

6.1 Construction of select groups

Group 6.1. $|G| = 4$

1. If there exists $g \in G$ with $o(g) = 4$, then $G \cong C_4$.
2. If there does not exist $g \in G$ with $o(g) = 4$, then $G \cong C_2 \times C_2$.

Group 6.2. $|G| = 6$

1. If there exists $g \in G$ with $o(g) = 6$, then $G \cong C_6$.
2. If there exist $a, b \in G$ with $o(a) = 3$, $o(b) = 2$, then $a^i = bab$. Then
  - **a.** If $i = 0$, $a = 1$, and contradiction.
  - **b.** If $i = 1$, there exists $g \in G$ with $o(g) = 6$ and case **1.** holds.
  - **c.** If $i = 2$, then $G \cong S_3$.

3. For all $a \in G$ except for 1_G, $o(a) = 2$ or 3.
  - **a.** For all $g \in G$ with $g \neq 1_G$, $o(g) = 3$. This leads to a contradiction.
  - **b.** For all $g \in G$ with $g \neq 1_G$, $o(g) = 2$. This also leads to a contradiction.

Group 6.3. $|G| = 8$

1. If there exists $g \in G$ with $o(g) = 8$, then $G \cong C_8$.
2. If there does not exist $g \in G$ with $o(g) = 4$, then $G \cong C_2 \times C_2 \times C_2$.

3. There exists $b \in G$ with $o(b) = 4$.

a. There exists $a \in G \setminus \langle b \rangle$ with $o(a) = 2$, and $aba^{-1} \in \langle b \rangle$, so $aba^{-1} = b^k$.

i. If $k = 1$, then $G \cong C_2 \times C_4$.

ii. If $k = 1$, then $aba^{-1} = b^4$, and contradiction.

iii. If $k = 3$, then $G \cong D_4$.

b. There does not exist $a \in G \setminus \langle b \rangle$ with $o(a) = 2$, so let $a \in G \setminus b$ with $o(a) = 4$. Then $aba^{-1} = b^k$.

i. If $k = 1$, then $o(ab) = 4$, and contradiction.

ii. If $k = 2$, then $b = 1$, and contradiction.

iii. If $k = 3$, then $G \cong Q$.

Group 6.4. $|G| = 12$

For $|G| = 12$, there exist $H, K \leqslant G$ with $|H| = 4$ and $|K| = 3$.

1. If $H, K \lhd G$, then $G \cong C_4 \times C_3 \cong C_{12}$ or $G \cong C_2 \times C_2 \times C_3 \cong C_6 \times C_2$.

2. If $H \lhd G$ and $H \cong C_4$, then all homomorphisms $\varphi : K \to \mathrm{Aut}(H)$ are trivial, and case **1.** holds.

3. If $H \lhd G$ and $H \cong C_2 \times C_2$, $\mathrm{Aut}(H) = S_3$, then $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K \cong G \cong A_4 \;\; \forall \;\; \varphi_1, \varphi_2 \in \mathrm{Aut}(H)$.

4. If $K \lhd G$ and $H \backsim C_2 \times C_2$, then $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K \cong G \cong D_6 \;\; \forall \;\; \varphi_1, \varphi_2 \in \mathrm{Aut}(H)$.

5. If $K \lhd G$ and $H \backsim C_4$, then $G \cong C_3 \rtimes C_4$.

6.2 Summary of groups up to order 23

Order	Number of isomorphism classes	Abelian groups	Non-abelian groups
1	1	C_1	–
2	1	C_2	–
3	1	C_3	–
4	2	$C_4, C_2 \times C_2$	–
5	1	C_5	–
6	2	C_6	S_3
7	1	C_7	–
8	5	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$	D_4, Q
9	2	$C_9, C_3 \times C_3$	–
10	2	C_{10}	D_5
11	1	C_{11}	–
12	5	$C_{12}, C_6 \times C_2$	$A_4, D_6, C_3 \rtimes C_4$
13	1	C_{13}	–
14	2	C_{14}	D_7
15	1	C_{15}	–
16	14	*Difficult to classify*	*Difficult to classify*
17	1	C_{17}	–
18	3	$C_{18}, C_6 \times C_3$	$D_9, S_3 \times C_3, (C_3 \times C_3) \rtimes C_2$
19	1	C_{19}	–
20	5	$C_{20}, C_{10} \times C_2$	$D_{10}, C_5 \rtimes C_4, F_{20}$
21	2	C_{21}	$C_7 \rtimes C_3$
22	2	C_{22}	D_{11}
23	1	C_{23}	–

The Frobenius group of order 20 F_{20} has been included only as a reference.

7 Selected proofs

Theorem 1.3.5. [Subgroup test]
Let G be a group and H a non-empty subset of G. Then

1. H is a subgroup of G if and only if for all $a, b \in H$, $ab^{-1} \in H$

2. If H is finite, H is a subgroup if and only if for all $a, b \in H$, $ab \in H$

Proof: **1.** Since H is nonempty, there exists $a \in H$.
Therefore $aa^{-1} \in H$
So $1 \in H$.
Therefore $1a^{-1} = a^{-1} \in H$
For all $a, b \in H$, $b^{-1} \in H$ and $a(b^{-1})^{-1} = ab \in H$
Therefore H is closed under multiplication.
So H is a group.

2. It is enough to show that for all $a, b \in H$, $a^{-1} \in H$.
For all $a, b \in H$, by the assumption $\{a, a^2, \dots\} = \{a^m \mid m \in \mathbb{N}\} \subseteq H$
Since H is finite, there are repeats.
So there exist $m_1 < m_2 \in \mathbb{N}$ such that $a^{m_1} = a^{m_2}$
So $a^{m_2 - m_1} = 1$ and $a^{m_2 - m_1 - 1} = a^{-1}$
Thus $a^{-1} \in H$.
Note if $m_2 = m_1 + 1$, then it follows that $a = 1$, so $a^{-1} \in H$ consequently. ∎

Proposition 1.3.6. Let G be a group and let $a, b \in G$ of finite order. Then

1. If $k \in \mathbb{N}$ and $a^k = 1$, then $o(a) \mid k$

2. If $k \in \mathbb{N}$, then $o(a^k) = \dfrac{o(a)}{(o(a), k)}$

3. If $(o(a), o(b)) = 1$ and $ab = ba$, then $o(ab) = o(a)o(b)$

Proof: **1.** Let $k = o(a)q + r$ for $0 \leqslant r < o(a)$.
Then $1 = a^k = a^{o(a)q}a^r = a^r$
By definition of r and minimality of $o(a)$, $r = 0$.
Therefore $o(a) \mid k$.

2. Let $n = o(a^k)$, $m = \frac{o(a)}{(k, o(a))}$.
Consider $(a^k)^{\frac{o(a)}{(k,o(a))}} = (a^{o(a)})^{\frac{o(a)}{(k,o(a))}} = 1$
Therefore $o(a^k) = n \leqslant \frac{o(a)}{(k,o(a))} = m$.
Note $1 = (a^k)^{o(a^k)} = a^{ko(a^k)}$
By **1.**, $o(a) \mid ko(a^k)$.
This implies $\frac{o(a)}{(k,o(a))} \mid \frac{ko(a^k)}{(k,o(a))}$
Since $\left(\frac{o(a)}{(k,o(a))}, \frac{k}{(k,o(a))}\right) = 1$, by Math 135 proposition, $\frac{o(a)}{(k,o(a))} \mid o(a^k)$.
Therefore $m \leqslant n$.
Therefore $m = n$.

3. Let $n' = o(ab)$, $m = o(a)o(b)$.
Then $(ab)^{o(a)o(b)} = abab \dots ab = a^{o(a)o(b)}b^{o(a)o(b)} = 1$
By minimality of $o(a), o(b)$, $n' \leqslant m'$.
Now consider $1 = (ab)^{o(ab)} = a^{o(ab)}b^{o(ab)} = a^{o(a)o(ab)}b^{o(a)o(ab)} = b^{o(a)o(ab)}$.
By **1.**, $o(b) \mid o(a)o(ab)$.
By a Math 135 proposition, since $(o(a), o(b)) = 1$, $o(b) \mid o(ab)$.
Similarly $o(a) \mid o(ab)$.

Since $(o(a), o(b)) = 1$, $o(a)o(b) \,\big|\, o(ab)$.
So $m' \leqslant n'$.
Therefore $m' = n'$. ∎

Theorem 1.3.7. A subgroup of a cyclic group is always cyclic.

Proof: Let $H \leqslant G$.
Let $\ell = \min\{n \,\big|\, g^n \in H, n \in \mathbb{N}\}$ for $H \neq \{1_G\}$.
Since $H \neq \{1_G\}$, there exists $n > 0$ such that $g^n = 1_G \in H$.
If $n > 0$, the set is well defined.
If $n < 0$, then since H is a subgroup, $(g^n)^{-1} = g^{-n} \in H$ and $-n \in \{n \,\big|\, g^n \in H, n \in \mathbb{N}\}$.
Hence the set is non-empty and well-defined.
Claim: $H = \left\langle g^\ell \right\rangle$ is cyclic and generated by g^ℓ.
Let $h \in H$ with $h = g^m$ for some $m \in \mathbb{Z}$.
By the division algorithm, $m = q\ell + r$ for $0 \leqslant r < \ell$.
Thus $g^m = g^{q\ell + r} = (g^\ell)^q g^r$ and $g^r = g^{m - q\ell} = g^m((g^\ell)^q)^{-1} \in H$.
And since $0 \leqslant r < \ell$, it must be that $r = 0$.
So $h = (g^\ell)^q \in \left\langle g^\ell \right\rangle$.
Therefore $H = \left\langle g^\ell \right\rangle$. ∎

Theorem 1.3.8. A finite cyclic group of order n has precisely one subgroup of order m for each $n \in \mathbb{N}$ such that $m \,\big|\, n$. These are the only subgroups of the given group.

Proof: Suppose $|G| = n < \infty$ and let $m \in \mathbb{N}$ such that $m \,\big|\, n$.
Let $\ell = \frac{n}{m}$ and $G = \langle g \rangle$.
Then $H = \left\langle g^\ell \right\rangle = \frac{o(g)}{(\ell, o(g))} = \frac{n}{(\ell, n)} = \frac{n}{\ell} = m$.
So $|\left\langle g^\ell \right\rangle| = o(g^\ell) = m$, and a subgroup of order m exists.
Let $H \leqslant G$ and $|H| = m > 1$ as above.
So $H = \langle g^e ll \rangle$ for $\ell = \min\{k \,\big|\, g^k \in H, k \in \mathbb{N}\}$.
Consider $n = q\ell + r$ for $0 \leqslant r < \ell$.
As in the above proof, by the minimality of ℓ, $r = 0$.
Thus $n = g\ell \implies \ell \,\big|\, n$.
So $|H| = |\left\langle g^\ell \right\rangle| = o(g^\ell) = \frac{o(g)}{(\ell, o(g))} = \frac{n}{\ell}$.
Therefore $m \,\big|\, n$.
Now suppose that $H' \leqslant G$ and $|H'| = |H| = m$.
Repeat the above argument with $H' = \left\langle g^{\ell'} \right\rangle$ for $\ell' = \min\{k \,\big|\, g^k \in H', k \in \mathbb{N}\}$.
Then $\ell' \,\big|\, n$ and $|H'| = \frac{n}{\ell'}$, which implies that $\ell = \ell'$.
Therefore $H = H'$. ∎

Theorem 1.4.9. [Lagrange]
If G is a group and H a subgroup of G, then $|H| \,\Big|\, |G|$. We denote $[G, H] = |G|/|H|$ to be the <u>index</u> of H.

Proof: For R a set of representatives of cosets of G, $G = \displaystyle\bigsqcup_{a_i \in R} Ha_i$.
Since $\varphi : H \to Ha$, defined by $h \mapsto ha$, is a bijection, $|H| = |H_{a_i}|$ for any $a_i \in R$.
So $|G| = \displaystyle\sum_{a_i \in R} |Ha_i| = \sum_{a_i \in R} |H| = |R||H|$.
Therefore $|H| \,\big|\, |G|$ and $|R|$ is the index of H in G. ∎

Proposition 2.3.2. Suppose G is a finite group with $H, K \leqslant G$. Then $|HK| = \dfrac{|H||K|}{|H \cap K|} = |KH|$

Proof: Define an equivalence relation $\sim$ on $H \times K = \{(h,k) \,\big|\, h \in H, k \in K\}$.
This relation is given by by $(h_1, k_1) \sim (h_2, k_2) \iff h_1k_1 = h_2k_2$.
Let P be the partition containing (h,k) and let $(h', k') \in P$.
Then $hk = h'k' \iff h'^{-1}h = k'k^{-1}$.
Let $\ell = h'^{-1}h = k'k^{-1}$.
Then $\ell = h'^{-1}h \in H$ and $\ell = k'k^{-1} \in K$, so $\ell \in H \cap K$.
Conversely, let $\ell \in H \cap K$ with $h' = h\ell^{-1}$ and $k' = \ell k$.
Thus $h'k' = hk$ so $(h', k') \sim (h, k)$.
So $P = \{(h', k') \,\big|\, \ell \in H \cap K, h' = h\ell^{-1}, k' = \ell k\}$.
By the law of cancellation, all pairs in P are distinct.
Therefore $|P| = |H \cap K|$.
Finally, $|HK| =$ the number of equivalence classes $= \dfrac{|H||K|}{|H \cap K|}$. ∎

Theorem 5.2.4. If A is abelian, then
1. $T(A) = \{a \in A \,\big|\, o(a) < \infty\}$ is termed the <u>torsion part</u> of A, and $T(A) \leqslant A$
2. ${}^{A}\!\big/_{T(A)}$ is torsion-free

Proof: **1.** Note that $0 \in T(A)$, so $T(A) \neq \emptyset$.
Let $a, b \in T(A)$, and observe that $o(b) = o(-b)$.
So $o(a)o(b)(a-b) = o(a)o(b)a - o(a)o(b)b = 0 \Longrightarrow o(a-b) \leqslant o(a)o(b) \Longrightarrow a - b \in T(A)$.
Thus by the subgroup test, $T(A) \leqslant A$.

2. Let $b \in {}^{A}\!\big/_{T(A)}$ such that there exists $n \in \mathbb{Z}$ with $n\bar{b} = \bar{0}$ in ${}^{A}\!\big/_{T(A)}$.
Here recall $\bar{b}$ means the image of b under the natural homomorphism from A to $T(A)$.
Since $n\bar{b} = \bar{0}$, $nb \in T(A)$.
Thus $o(nb) < \infty$ and $o(nb)nb = 0$.
So there exists $b \in T(A)$ with $\bar{b} = \bar{0}$. ∎

References

Badawi, Ayman. *Abstract Algebra Manual: Problems and Solutions.* Nova Science: 2004
Dummit, David S. and Richard M. Foote. *Abstract Algebra.* Wiley: 1999
Papantonopoulou, Aigli. *Algebra: Pure and Applied.* Prentice Hall: 2001