Contents

1 Basic Definitions

1.1 Definitions

Definition 1.1. A *group* is a set G together with a binary operation $*$:

$$(a, b) \mapsto a * b : G \times G \to G$$

satisfying the following

1. for all $a, b, c \in G$,
$$(a * b) * c = a * (b * c).$$

2. there exists an element(called *neutral element*) $e \in G$ such that
$$a * e = a = e * a$$
for all $a \in G$.

3. for each $a \in G$, there exists an $a' \in G$(called *inverse* of a, and denoted it a^{-1}) such that
$$a * a' = e = a' * a.$$

Remark 1.2. The group conditions 2. and 3. can be replaced by the following weaker conditions:

- there exists an e such that $e * a = a$ for all a.

- for each $a \in G$, there exits an $a' \in G$ such that $a' * a = e$.

Definition 1.3. 1. A set S together with a binary operation $(a, b) \mapsto a \cdot b : S \times S \to S$ is called a *magma*.

2. When the binary operation is associative, $(S, \cdot)$ is called a *semigroup*.

3. A semigroup with a neutral element is called a *monoid*.

Definition 1.4. 1. The *order* $|G|$ of a group G is its cardinality.

2. A finite group whose order is a power of a prime p is called a *p-group*.

3. For an element a of a group G, define

$$a^n = \begin{cases} \underbrace{aa \cdots a}_{n\text{copies}} & n > 0 \\ e & n = 0 \\ \underbrace{a^{-1}a^{-1} \cdots a^{-1}}_{n\text{copies}} & n < 0 \end{cases}$$

4. The set $\{n \in \mathbb{Z} : a^n = e\}$ is an ideal in $\mathbb{Z}$, and so equals $m\mathbb{Z}$ for some integer $m \geq 0$.
   - When $m = 0, a^n = e$ unless $n = 0$, and a is said to have *infinite order*.
   - When $m \neq 0$, it is the smallest integer $m > 0$ such that $a^m = e$, and a is said to have *finite order m*.

Definition 1.5. When G and H are groups, we can construct a new group $G \times H$, called the *direct product* of G and H. As a set, it is the Cartesian product of G and H, and multiplication is defined by

$$(g, h)(g', h') := (gg', hh').$$

Definition 1.6. A group G is *commutative*(or *abelian*) if

$$ab = ba, \text{ all } a, b \in G.$$

1.2 Subgroups

Definition 1.7. Let S be a nonempty subset of a group G. If

1. $a, b \in S \implies ab \in S$, and
2. $a \in S \implies a^{-1} \in S$,

then the binary operation on G makes S into a group, called a *subgroup* of G.

Remark 1.8. When S is finite, condition 1. implies 2..

Definition 1.9. The *centre* of a group G is the subset

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

It is a subgroup of G.

Definition 1.10. In a commutative group G, the elements of finite order form a subgroup G_{tor} of G, called the *torsion subgroup*.

Proposition 1.11. *An intersection of subgroups of G is a subgroup of G.*

Example 1.12. However, the product of subgroup need NOT to be a subgroup, consider $G = S_3, U = (13), V = (12)$.

Proposition 1.13. *For any subset X of a group G, there is a smalleset subgroup of G containing X. It consists of all finite products of elements of X and their inverses.*

Definition 1.14. The subgroup S in the above proposition is denoted $\langle X\rangle$, and is called the *subgroup generated* by X. In particular, $\langle\emptyset\rangle = \{e\}$. We say that X *generates* if $G = \langle X\rangle$.

Definition 1.15. For a subset S of a group G and an element a of G, we let

$$aS = \{as : s \in S\}, \quad Sa = \{sa : s \in S\}.$$

When H is a subgroup of G, the sets of the form aH are called the *left cosets* of H in G, and the sets of the form Ha are called the *right cosets* of H in G.

Proposition 1.16. *Let H be a subgroup of a group G.*

1. *An element a of 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 coset have the same number of elements.*

Definition 1.17. The *index* $(G : H)$ of H in G is defined to be the number of left cosets of H in G. In particular, $(G : 1)$ is the order of G.

Theorem 1.18 (Lagrange)**.** *If G is finite, then*

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

In particular, the order of every subgroup of a finite group divides the order of the group.

Remark 1.19. Lagrange's theorem has partial converses:

1. (Cauchy's theorem)if a prime p divides $m = (G : 1)$, then G has an element of order p.
2. (Sylow's theorem)if a prime power p^n divides m, then G has a subgroup of order p^n.

However, Klein 4-group $C_2 \times C_2$ has no element of order 4; A_4 has order 12, but has no subgroup of order 6.

Corollary 1.20. *The order of each element of a finite group divides the order of the group.*

Proposition 1.21. *For any subgroups $H \supseteq K$ of G,*

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

(meaning either both are infinite or both are finite and equal).

Proof. Write $G = \sqcup_{i\in I} g_i H$ and $H = \sqcup_{j\in J} h_j K$, then $G = \sqcup_{i,j\in I\times J} g_i h_j K$. □

1.3 Normal Subgroups

Definition 1.22. A subgroup N of G is *normal*, denoted $N \lhd G$, if $gNg^{-1} = N$ for all $g \in G$.

Remark 1.23. To show that N is normal, it suffices to check that $gNg^{-1} \subseteq N$ for all g, because it implies that $N \subseteq g^{-1}Ng$, and rewriting this with gives that $N \subseteq gNg^{-1}$ for all g. However, the next example shows that there can exist a subgroup N of a group G and an element g of G such that $gNg^{-1} \subseteq N$ but $gNg^{-1} \neq N$.

Example 1.24. Let $G = \mathrm{GL}_2(\mathbb{Q})$, and let $H = \left\{\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} : n \in \mathbb{Z}\right\}$. Then H is a subgroup of G and $H \simeq \mathbb{Z}$. Let $g = \begin{pmatrix}5 & 0\\ 0 & 1\end{pmatrix}$. Then

$$g\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}g^{-1} = \begin{pmatrix}1 & 5n\\ 0 & 1\end{pmatrix}$$

Hence $gHg^{-1} \subsetneq H$.

Proposition 1.25. *A subgroup N of G is normal $\iff$ every left coset of N in G is also a right coset, in which case, $gN = Ng$ for all $g \in G$.*

Proposition 1.26. *Every subgroup of index two is normal.*

Proof. Indeed, let $g \in G \backslash H$. Then $G = H \sqcup gH$. It implies that gH and Hg are the complements of H in G, and hence they are equal. □

Example 1.27. Consider the dihedral group

$$D_n = \left\{e, r, \cdots, r^{n-1}, s, \cdots, r^{n-1}s\right\}.$$

Then $C_n = \left\{e, r, \cdots, r^{n-1}\right\}$ has index 2 and hence is normal. For $n \geq 2$, the subgroup $\{e, s\}$ is not normal because $r^{-1}sr = r^{n-2}s \notin \{e, s\}$.

Similar to 1.11, we have

Proposition 1.28. *An 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.*

In 1.12, we found that the product of subgroups need not to be a subgroup. If we enhance the condition to normal subgroup, then the statement will be true.

Theorem 1.29. *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.*

Like 1.13, we want to generate a normal subgroup by a subset. In order to do this, we need more preparations.

Definition 1.30. We say that a subset X of a group G is *normal* if $gXg^{-1} \subseteq X$ for all $g \in G$.

Lemma 1.31.
1. *If X is normal, then the subgroup $\langle X \rangle$ is normal.*
2. *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 1.32. *The normal subgroup generated by a subset X of G is $\left\langle \bigcup_{g \in G} gXg^{-1} \right\rangle$.*

We can give another result about the largest normal subgroup contained in a given subgroup.

Lemma 1.33. *For any subgroup H of a group G, $\bigcap_{g \in G} gHg^{-1}$ is the largest normal subgroup of G contained in H.*

1.4 Examples

Definition 1.34. A group is said to be *cyclic* if it is generated by a single element, i.e. if $G = \langle r \rangle$ for some $r \in G$.

If r has finite order n, then

$$G = \left\{e, r, r^2, \cdots, r^{n-1}\right\} \simeq C_n, \quad r^i \leftrightarrow i \mod n,$$

and G can be thought of as the group of rotational symmetries about the centre of a regular polygon with n-sides. If r has infinitely order, then

$$G = \left\{\cdots, r^{-i}, \cdots, r^{-1}, \cdots, e, r, r, \cdots, r^i, \cdots\right\} \simeq C_\infty, \quad r^i \leftrightarrow i.$$

Thus, up to isomorphism, there is exactly one cyclic group of order n for each $n \leq \infty$.

Proposition 1.35. *Let $G = \langle a \rangle$ be a cyclic group of order n. Then the generators of G are exactly the elements a^m with $\gcd(m, n) = 1$, where $m \geq 1$.*

Example 1.36. The units of finite field form a cyclic group. In particular, $\mathbb{F}_p^\times$ is cyclic for some prime.

Proof. 1.56. □

1.5 Homomorphisms

Definition 1.37. A *homomorphism* from a group G to a second G' is a map $\alpha : G \to G'$ such that $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in G$. An *isomorphism* is a bijective homomorphism.

Theorem 1.38 (Cayley)**.** *There is a canonical injective homomorphism*

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

Corollary 1.39. *A finite group of order n can be realized as a subgroup of S_n.*

Definition 1.40. The *kernel* of a homomorphism $\alpha : G \to G$" is

$$\ker(\alpha) = \{g \in G : \alpha(g) = e\}.$$

Proposition 1.41. *1. α is injective $\iff \ker(\alpha) = \{e\}$.*

2. The kernel of a homomorphism is a normal subgroup.

Example 1.42. The kernel of the homomorphism $\det : \mathrm{GL}_n(F) \to F^\times$ is the group of $n \times n$ matrics with determinant 1, this group $\mathrm{SL}_n(F)$ is called the *special linear group* of *degree n*.

Proposition 1.43. *Every normal subgroup occurs as the kernel of a homomorphism. More precisely, if N is a normal subgroup of G, then there is a unique group structure on the set G/N of cosets of N in G for which the natrual map*

$$a \mapsto [a] : G \to G/N$$

is a homomorphism. The group G/N is called the quotient *of G by N.*

Proposition 1.44. *The map $a \mapsto aN : G \to G/N$ has the following universal property: for any homomorphism $\alpha : G \to G'$ of groups such that $\alpha(N) = \{e\}$, there exists a unique homomorphism $G/N \to G'$ making the diagram commute.*

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

Theorem 1.45. *For any homomorphism $\alpha : G \to G'$ of groups, the kernel N of α is a normal subgroup of G, the image I of α is a subgroup of G', and α factors in a natural way into the composite of a surjection, an isomorphism, and an injection:*

$$G \longrightarrow G/N \longrightarrow I \longrightarrow G'$$

Theorem 1.46. *Let Hb e a subgroup of G and N a normal subgroup of G. Then HN is a subgroup of G, $H \cap N$ is a normal subgroup of H, and the map*

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

is an isomorphism.

Theorem 1.47. *Let $\alpha : G \twoheadrightarrow \widetilde{G}$ be a surjective homomorphism, and let $N = \ker(\alpha)$. Then there is a one-to-one correspondence*

$$\{\textit{subgroup of } G \textit{ containing } N\} \overset{1:1}{\leftrightarrow} \left\{\textit{subgroups of } \widetilde{G}\right\}$$

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

1. *$\widetilde{H} \subseteq \widetilde{H}' \iff H \subseteq H'$, in which case $(\widetilde{H}' : \widetilde{H}) = (H' : H)$;*

2. *$\widetilde{H}$ is normal in $\widetilde{G} \iff H$ is normal in G, in which case, α induces an isomorphism*

$$G/H \simeq \widetilde{G}/\widetilde{H}.$$

Corollary 1.48. *Let N be a normal subgroup of G.*

1. *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*
2. *Moreover, H is normal in $G \iff H/N$ is normal in G/N, in which case the homomorphism $g \mapsto gN : G \to G/N$ induces an isomorphism*

$$G/H \simeq (G/N)/(H/N).$$

1.6 Direct Products

We now give a generalization of 1.5:

Definition 1.49. Let G be a group, and let $H_1, \cdots, H_k$ be subgroups of G. We says that G is a *direct product* of the subgroups H_i if the map

$$H_1 \times H_2 \times \cdots \times H_k \to G : (h_1, h_2, \cdots, h_k) \mapsto h_1 h_2 \cdots h_k$$

is an isomorphism of groups.

Remark 1.50. This means that each element g of G can be written uniquely in the form $g = h_1 h_2 \cdots h_k, h_i \in H_i$, and that if $g = h_1 h_2 \cdots h_k$ and $g' = h_1' h_2' \cdots h_k'$, then

$$gg' = (h_1 h_1')(h_2 h_2') \cdots (h_k h_k').$$

Proposition 1.51. *A group G is a direct product of subgroups H_1, H_2 if and only if*

1. *$G = H_1 H_2$,*
2. *$H_1 \cap H_2 = \{e\}$,*
3. *One of the followings holds:*
   (a) *every element of H_1 commutes with every element of H_2.*
   (b) *H_1 and H_2 are both normal in G.*

Proposition 1.52. *A group G is a direct product of subgroups $H_1, H_2, \cdots, H_k$ if and only if*

1. *$G = H_1 H_2 \cdots H_k$,*
2. *for each j, $H_j \cap (H_1 \cdots H_{j-1} H_{j+1} \cdots H_k) = \{e\}$,*
3. *each of $H_1, H_2, \cdots, H_k$ is normal in G.*

1.7 Commutative Groups

In this subsection, let M be a commutative group, written additively. The subgroup $\langle x_1, \cdots, x_k \rangle$ of M generated by the elements $x_1, \cdots, x_k$ consists of the sums $\sum m_i x_i, m_i \in \mathbb{Z}$.

Definition 1.53. A subset $\{x_1, \cdots, x_k\}$ of M is a *basis* for M if it generates M and

$$m_1 x_1 + \cdots + m_k x_k = 0, \quad m_i \in \mathbb{Z} \implies m_i x_i = 0 \text{ for every } i$$

then

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

Lemma 1.54. *Let $x_1, \cdots, x_k$ generate M. For any $c_1, \cdots, c_k \in \mathbb{N}$ with $\gcd(c_1, \cdots, c_k) = 1$, there exists generators $y_1, \cdots, y_k$ for M such that $y_1 = c_1 x_1 + \cdots + c_k x_k$.*

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

- $\{x_1, x_2 + x_1, x_3, \cdots, x_k\}$ generates M.

- $\gcd(c_1 - c_2, c_2, c_3, \cdots, c_k) = 1$,
- $(c_1 - c_2) + c_2 + \cdots + c_k < s$,

and so, by induction, there exist generators $y_1, \cdots, y_k$ for M with

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

□

Theorem 1.55. *Every finitely generated commutative group M has a basis; hence it is a finite direct sum of cyclic group.*

Proof. We argue by induction on the number of generators of M. If M can be generated by one element, the statement is trivial, and so we may assume that it requires at least $k > 1$ generators. Among the generating sets $\{x_1, \cdots, x_k\}$ for M with k elements there is one for which the order of x_1 is the smallest possible.

We claim that M is then the direct sum of $\langle x_1 \rangle$ and $\langle x_2, \cdots, x_k \rangle$, then the proof is completed by induction. If M is not the direct sum of $\langle x_1 \rangle$ and $\langle x_2, \cdots, x_k \rangle$, then there exists a relation

$$m_1x_1 + m_2x_2 + \cdots + m_kx_k = 0$$

with $m_1x_1 \neq 0$. After possibly changing the sign of some of the x_i, we may suppose that $m_1, \cdots, m_k \in \mathbb{Z}_{\geq 0}$ and $m_1 < \mathrm{order}(x_1)$. Let $d = \gcd(m_1, \cdots, m_k) > 0$ and let $c_i = m_i/d$. According to the 1.54, there exists a generating set $y_1, \cdots, y_k$ such that $y_1 = c_1x_1 + \cdots + c_kx_k$. But

$$dy_1 = m_1x_1 + m_2x_2 + \cdots + m_kx_k = 0$$

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

The following corollary can be used to show the units of a finite field is a cyclic group.

Corollary 1.56. *A finite commutative group is cyclic if, for each $n > 0$, it contains at most n elements of order dividing n.*

Proof. By 1.55, we can now suppose that $G = C_{n_1} \times \cdots \times C_{n_r}$ for $n_i \in \mathbb{Z}_{>0}$. If n divides n_i and n_j with $i \neq j$, then G has more than n elements of order dividing n. Therefore, the hypothesis implies that the n_i are relatively prime. Let a_i generate the ith factor. Then $(a_1 \cdots a_r)$ has order $n_1 \cdots n_r$, and so generates G. □

Theorem 1.57. *A nonzero finitely generated commutative group M can be expressed*

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

for certain integers $n_1, \cdots, n_s \geq 2$ 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 $n_1 \mid n_2, \cdots, n_{s-1} \mid n_s$, 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. In other words, M can be expressed*

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

for certain prime power $p_i^{e_i}$ (repetitions of primes allowed) uniquely determined by M.

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

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

and so r is the dimension of M/pM as an $\mathbb{F}_p$-vector space.

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

$$C_m \times C_n \simeq C_{mn}.$$

  Use the above equation to decompose the C_{n_i} into products of cyclic groups of prime power order. Once this has been achieved, it can be used to combine factors to achieve a decomposition as in (2): for example, $C_{n_s} = \prod C_{p_i^{e_i}}$, where the product is over the distinct primes among the p_i and e_i is the highest exponent for the prime p_i.

  In proving the uniqueness statements, we can replace M with its torsion subgroup(and so assume $r=0$). A prime p will occur as one of the primes p_i in 1 $\iff$ M has an element of order p, in which case p will occur exactly a times, where p^a is the number of elements of order dividing p. Similarly, p^2 will divide some $p_i^{e_i}$ in 1 $\iff$ M has an element of order p^2, in which case it will divide exactly b of the $p_i^{e_i}$, where $p^{a-b}p^{2b}$ is the number of elements in M of order dividing p^2. Continuing in this fashion, we find that the elementary divisors of M can be read off from knowing the numbers of elements of M of each prime power order.

  The uniqueness of the invariant factors can be derived from that of the elementary divisors.

□

Definition 1.58. In 1.57,

- The number r is called the *rank* of M.
- $n_1, \cdots, n_s$ are called the *invariant factors* of M.
- $p_1^{e_1}, \cdots, p_t^{e_t}$ are called the *elementary divisors* of M.

1.8 Dual Groups

Let $\mu(\mathbb{C}) = \{z \in \mathbb{C} : |z| = 1\}$. Then $\mu(\mathbb{C})$ is an infinite group. For any integer n, the set $\mu_n(\mathbb{C})$ of elements of orer dividing n is cycle of order n, i.e.

$$\mu_n(\mathbb{C}) := \left\{e^{2\pi i m/n} : 0 \le m \le n-1\right\} = \left\{1, \xi, \cdots, \xi^{n-1}\right\},$$

where $\xi = e^{2\pi i/n}$ is a primitive nth root of 1.

Definition 1.59. 1. A *linear character*(or just *character*) of a group G is a homomorphism $G \to \mu(\mathbb{C})$.

2. The homomorphism $a \mapsto 1$ is called the *trivial* (or *principal*) *character*.

Example 1.60. The *Legendre symbol* modulo p of an integer a not divisible by p is

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{Z}/p\mathbb{Z} \\ -1 & \text{otherwise} \end{cases}.$$

Clearly, this depends only on a modulo p. If neither a nor b is divisible by p, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$: suppose that $p \neq 2$; then it follows from $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group by 1.36 and if $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ are generators, then $b = a^n$ for some odd number n (or else, $a = a^m$ for some even number m, but $(\mathbb{Z}/p\mathbb{Z})^\times$ with an even order $p-1$ contradicting with 1.35). Therefore $[a] \mapsto \left(\frac{a}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\} = \mu_2(\mathbb{C})$ is a character of $(\mathbb{Z}/p\mathbb{Z})^\times$, sometimes called the quadratic character.

Definition 1.61. The set of characters of a group G becomes a group $G^\vee$ under the addition,

$$(\chi + \chi')(g) := \chi(g)\chi'(g),$$

called the *dual group* of G. For example, the dual group $\mathbb{Z}^\vee$ of $\mathbb{Z}$ is isomorphic to $\mu(\mathbb{C})$ by the map $\chi \mapsto \chi(1)$.

Theorem 1.62. *Let G be a finite commutative group.*

1. *The dual of $G^\vee$ is isomorphic to G.*
2. *The map $G \to G^{\vee\vee}$ sending an element a of G to the character $\chi \to \chi(a)$ of $G^\vee$ is an isomorphism.*

In other words, $G \simeq G^\vee$ and $G \simeq G^{\vee\vee}$.

Proof. The statement is obvious for cyclic groups. By 1.55, it suffices to see that $(G \times H)^\vee \simeq G^\vee \times H^\vee$. And the homomorphism below is bijective.

$$\chi \mapsto (\chi_1, \chi_2), \quad (G \times H)^\vee \to G^\vee \times H^\vee,$$

where $\chi_1(g) = \chi(g, e)$ and $\chi_2(h) = \chi(e, h)$. □

Theorem 1.63. *Let G be a finite commutative group. For any characters χ and ψ of G,*

$$\sum_{a \in G} \chi(a)\psi(a^{-1}) = \begin{cases} |G| & \text{if } \chi = \psi, \\ 0 & \text{otherwise} \end{cases}.$$

In particular,

$$\sum_{a \in G} \chi(a) = \begin{cases} |G| & \text{if } \chi \text{ is trivial} \\ 0 & \text{otherwise} \end{cases}.$$

Proof. If $\chi = \psi$, then $\chi(a)\psi(a^{-1}) = 1$, and so the sum is $|G|$. Otherwise there exists a $b \in G$ such that $\chi(b) \neq \psi(b)$. As a runs over G, so also does ab and so

$$\sum_{a \in G} \chi(a)\psi(a^{-1}) = \sum_{a \in G} \chi(ab)\psi((ab)^{-1}) = \chi(b)\psi(b)^{-1} \sum_{a \in G} \chi(a)\psi(a^{-1}).$$

Because $\chi(b)\psi(b)^{-1} \neq 1$, this implies that $\sum_{a \in G} \chi(a)\psi(a^{-1}) = 0$. □

Corollary 1.64. *For any $a \in G$,*

$$\sum_{\chi \in G^\vee} \chi(a) = \begin{cases} |G| & \text{if } a = e \\ 0 & \text{otherwise} \end{cases}.$$

1.9 Order of elements

Proposition 1.65. *Let a, b be two elements with finite orders in a group with $ab = ba$, then $|ab| =$* $\gcd(a, b)$*.*

Theorem 1.66. *For any integers $m, n, r > 1$, there exists a finite group G with elements a and b such that a has order m, b has order n, and ab has order r.*

1.10 Groups of small order

In the following table, $c + n = t$ means that there are c commutative groups and n noncommutative groups.

$\lvert G\rvert$	$c + n = t$	Groups
4	$2 + 0 = 2$	$C_4, C_2 \times C_2$
6	$1 + 1 = 2$	$C_6; S_3$

2 Free Groups

2.1 Free Monoid

Definition 2.1. Let $X = \{a, b, c, \cdots\}$ be a set of symbols. A *word* is a finite sequence of symbols from X in which repetition is allowed. For example,

$$aa, \quad aabac, \quad b$$

are distinct words. Two words can be ultiplied by *juxtaposition*, for example,

$$aaaa * aabac = aaaaaabac.$$

This defines on the set of all words an associative binary operation. The empty sequence is allowed, and we denoted it by 1. Then 1 serves as an identity element. Write SX for the set of words together with this binary operation. Then SX is a monoid, called the *free monoid* on X.

Proposition 2.2. *When we identify an element a of X with the word a, X becomes a subset of SX and generates it, i.e. no proper submonoid of SX contains X. Moreover, the map $X \to SX$ has the following universal property: for any map of sets $\alpha : X \to S$ from X to a monoid S, there exists a unique homomorphism $SX \to S$ making the diagram commute.*

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

2.2 Free Group

We want to construct a group FX containing X and having the same universal property as SX with "monoid" replaced by "group". Define X' to be the set consisting of the symbols in X and also one addition symbol, denoted a^{-1}, for each $a \in X$; thus

$$X' = \left\{a, a^{-1}, b, b^{-1}, \cdots\right\}.$$

Let W' be the set of words using symbols from X'. This becomes a monoid under juxtaposition, but it is not a group because a^{-1} is not yet the inverse of a, and we can't cancel out the obvious terms in words of the following form:

$$\cdots aa^{-1} \cdots \text{ or } \cdots a^{-1}a \cdots$$

Definition 2.3. A word is said to be *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(possibly empty), which will be called the *reduced form* w_0 of w. There may be many different ways of performing the cancellations, for example

$$ca\underline{bb^{-1}}a^{-1}c^{-1}ca \to c\underline{aa^{-1}}c^{-1}ca \to \underline{cc^{-1}}ca \to ca$$
$$cabb^{-1}a^{-1}\underline{c^{-1}c}a \to cabb^{-1}\underline{a^{-1}a} \to ca\underline{bb^{-1}} \to ca.$$

We ended up with the same answer, and the next result says that this always happens.

Proposition 2.4. *There is only one reduced form of a word.*

Proof. Use induction on the length of the word w. Assume that w is not reduced and a pair of the form $a_0a_0^{-1}$ occurs. Observe that

1. Any two reduced forms of w obtained by a sequence of cancellations in which $a_0a_0^{-1}$ is cancelled first are equal by induction.

2. Any two reduced forms of w obtained by a sequence of cancellations in which $a_0a_0^{-1}$ is cancelled at some point are equal, because the result of such a sequence of cancellations will not be affected if $a_0a_0^{-1}$ is cancelled first.

3. Finally, consider a reduced form w_0 obtained by a sequence in which no cancellation cancels $a_0a_0^{-1}$ directly. Since $a_0a_0^{-1}$ does not remain in w_0, at least one of a_0 or a_0^{-1} must be cancelled at some point. If the pair itself is not cancelled, then the first cancellation involving the pair must look like

$$\cdots \cancel{a_0}^{-1}\overline{\cancel{a_0}a_0^{-1}}\cdots \text{ or } \cdots \underline{a_0\ \cancel{a_0}^{-1}}\ \cancel{a_0}\cdots .$$

But the word obtained after this cancellation is the same as if our original pair were cancelled, and so we may cancel the original pair instead.

□

Definition 2.5. We say two words w, w' are *equivalent*, denoted $w \sim w'$, if they have the same reduced form. This is an equivalence relation.

Proposition 2.6. *Products of equivalent words are equivalent, i.e.,*

$$w \sim w', \quad v \sim v' \implies wv \sim w'v'.$$

Definition 2.7. Let FX be the set of equivalence classes of words. Then FX is a group, called the *free group* on X.

Proposition 2.8. *For any maps of sets $\alpha : X \to G$ from X to a group G, there exists a unique homomorphism $FX \to G$ making the following diagram commute:*

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

Corollary 2.9. *Every group is a quotient of a free group.*

Theorem 2.10 (Nielsen-Schreier)**.** *Subgroups of free group are free.*

Two free groups FX and FY are isomorphic $\iff$ X and Y have the same cardinality. Thus we can define the *rank* of a free group G to be the cardinality of any free generating set, where a *free generating set* is a subset X of G for which the homomorphism $FX \to G$ given by 2.8 is an isomorphism.

Let H be a finitely generated subgroup of a free group G. Then there is an algorithm for constructing from any finite set of generators for H a free finite set of generators. If G has finite rank n and $(G : H) = i < \infty$, then H is free of rank

$$ni - i + 1.$$

In particular, H may have rank greater than that of G.

2.3 Generators and relations

Consider a set X and a set R of words made up of symbols in X.

Definition 2.11. 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*(or as a *set of defining relations*). One also says that (X, R) is a *presentation* for G, and denoted by $\langle X \mid R\rangle$.

Example 2.12. The dihendral group D_n has generators r, s and defining relations

$$r^n, s^2, srsr.$$

Example 2.13. The *generalized quaternion group Q_n*, $n \geq 3$, has generators a, b and relations

$$a^{2^{n-1}} = 1, a^{2^{n-2}} = b^2, bab^{-1} = a^{-1}.$$

It has order 2^n.

Proposition 2.14. *Let G be the group defined by the presentation (X, R). For any group H and map of sets $\alpha : X \to H$ sending each element of R to 1, there exists a unique homomorphism $G \to H$ making the following diagram commute:*

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

Proof. By 2.8, we know that α can be extended to a homomorphism $FX \to H$, which we denote again α. Then the normal subgroup N generated by ιR is contained in $\ker \alpha$. Finally apply 1.44. □

Example 2.15. Let $G = \{a, b \mid a^n, b^2, baba\}$. We prove that G is isomorphic to the dihedral group D_n: the map

$$\{a, b\} \to D_n, \quad a \mapsto r, \quad b \mapsto s$$

extends uniquely to a homomorphism $G \to D_n$.

3 Automorphisms and Extensions

3.1 Automorphisms of groups

Definition 3.1. An *automorphism* of a group G is an isomorphism of the group with itself. The set $\mathrm{Aut}(G)$ of automorphisms of G becomes a group under composition.

Definition 3.2. For $g \in G$, the map i_g "conjugation by g"

$$x \mapsto gxg^{-1} : \quad G \to G$$

is an automorphism of G. An automorphism of this form is called an *inner automorphism*, and the remaining automorphisms are said to be *outer*.

Proposition 3.3. *1.* $G/Z(G) \simeq \mathrm{Inn}(G)$*.*

2. $\mathrm{Inn}(G)$ *is a normal subgroup of* $\mathrm{Aut}(G)$

Proof. 1. $(gh)x(gh)^{-1} = g(hxh^{-1})g^{-1}$, i.e. $i_{gh}(x) = (i_g \circ i_h)(x)$, and so the map $g \mapsto i_g : G \to \mathrm{Aut}(G)$ is a homomorphism, with kernel $Z(G)$.

2. for $g \in G$ and $\alpha \in \mathrm{Aut}(G)$, we have $\alpha \circ i_g \circ \alpha^{-1} = i_{\alpha(g)}$.

□

Example 3.4. Let $G = (\mathbb{F}_p^n, +)$. The automorphisms of G as a commutative group are just the automorphisms of G as a vector space over $\mathbb{F}_p$. Thus $\mathrm{Aut}(G) = \mathrm{GL}_n(\mathbb{F}_p)$. Because G is commutative, all nontrivial automorphisms of G are outer. In particular, $\mathrm{Aut}(C_2 \times C_2) \simeq \mathrm{GL}_2(\mathbb{F}_2)$.

Example 3.5. As the centre of the quaternion group Q is $\langle a^2 \rangle$,

$$\mathrm{Inn}(Q) \simeq Q/\langle a^2 \rangle \simeq C_2 \times C_2.$$

In fact, $\mathrm{Aut}(Q) \simeq S_4$.

3.2 Automorphisms of Cyclic Groups

Let G be a finite cyclic group with order n. An automorphism α of G must send α to another generator of G, and so $\alpha(a) = a^m$ for some m relatively prime to n, by 1.35. The map $\alpha \mapsto m$ defines an isomorphism

$$\mathrm{Aut}(C_n) \to (\mathbb{Z}/n\mathbb{Z})^\times,$$

where

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\text{units in the ring } \mathbb{Z}/n\mathbb{Z}\} = \{m + n\mathbb{Z} : \gcd(m, n) = 1\}.$$

It remains to determine $(\mathbb{Z}/n\mathbb{Z})^\times$. If $n = p_1^{r_1} \cdots p_s^{r_s}$ is the factorization of n into a product of powers distinct primes, then

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{r_s}\mathbb{Z}, \quad m \mod n \leftrightarrow (m \mod p_1^{r_1}, \cdots, n \mod p_s^{r_s})$$

by Chinese Remainder Theorem. And so

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{r_s}\mathbb{Z})^\times.$$

It remains to consider the case $n = p^r$, where p is prime. $(\mathbb{Z}/p^r\mathbb{Z})^\times$ has order $p^{r-1}(p-1)$. The homomorphism

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$

is surjective with kernel of order p^{r-1}, and we know that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic by 1.36. Let $a \in (\mathbb{Z}/p^r\mathbb{Z})^\times$ map to a generators of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $a^{p^r(p-1)} = \left(a^{p^{r-1}(p-1)}\right)^p = 1$. And $a^{p^r} \neq 1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, hence a^{p^r} again maps to a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Therefore, $(\mathbb{Z}/p^r\mathbb{Z})^\times$ contains an element $\xi := a^{p^r}$ of order $p-1$. By 3.7, we have that $1+p$ has order p^{r-1} in $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Therefore $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic with generator $\xi \cdot (1+p)$ and every element can be written uniquely in the form

$$\xi^i \cdot (1+p)^j, \quad 0 \leq i < p-1, \quad 0 \leq j < p^{r-1}.$$

On the other hand,

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} = \langle \bar{3}, \bar{5} \rangle \simeq C_2 \times C_2$$

is not cyclic.

In summary, we have(For $p = 2$, see 3.8)

Theorem 3.6. *1. For a cyclic group of G of order n,* $\mathrm{Aut}(G) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$*. The automorphism of G of G corresponding to $[m] \in (\mathbb{Z}/n\mathbb{Z})^\times$ is $a \mapsto a^m$.*

2. If $n = p_1^{r_1} \cdots p_s^{r_s}$ with the p_i distinct primes, then

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{r_r}\mathbb{Z})^\times, \quad m \mod n \leftrightarrow (m \mod p_1^{r_1}, \cdots, m \mod p_s^{r_s}).$$

3. For a prime p,

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \simeq \begin{cases} C_{(p-1)p^{r-1}} & p \text{ odd} \\ C_2 & p^r = 2^2 \\ C_2 \times C_{2^{r-2}} & p = 2, r > 2. \end{cases}$$

Lemma 3.7. *1. Let n and k be integers, with $n \geq 2$ and $k \geq 0$. Then*

$$(1+n)^{n^k} \equiv 1 \pmod{n^{k+1}}.$$

2. If p is an odd prime, then

$$(1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}$$

for every positive integer k.

3. If p is an odd prime, then

$$(1+p)^{p^k} \not\equiv 1 \pmod{p^{k+2}}$$

for all $k \geq 0$.

4. Let p be an odd prime, and n positive integer. Then the order of $\overline{1+p} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ is p^{n-1}.

Proof. stackexchange □

Lemma 3.8. *1. $(1+4)^{2^{n-3}} \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ and the element 5 has order 2^{n-2} for $n \geq 2$.*

2. 5 and -1 generate the group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

3. $-1 \notin \langle 5 \rangle$.

4. $(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$.

Proof. stackexchange □

Definition 3.9. A *characteristic subgroup* of a group G is a subgroup H such that $\alpha(H) = H$ for all automorphisms α of G.

Remark 3.10. Like 1.23, to show H is a subgroup is to check that $\alpha(H) \subseteq H$ for all $\alpha \in \mathrm{Aut}(G)$. Moreover, a subgroup H of G is normal if it is stable under all *inner automorphisms* of G, and it is characteristic if it is stable under all automorphisms. In particular, a characteristic subgroup is normal.

Remark 3.11. Consider a group G and a normal subgroup N. An inner automorphism of G restricts to an automorphism of N, which may be outer. Thus a normal subgroup of N need not be a normal subgroup of G. However, a characteristic subgroup of N will be a normal subgroup of G. Also a characteristic subgroup of a characteristic subgroup is a characteristic subgroup.

Example 3.12. The centre $Z(G)$ of G is a characteristic subgroup.

Example 3.13. If H is the only nontrivial subgroup of G, then it must be characteristic.

Every subgroup of a commutative group is normal but not necessarily characteristic.

Example 3.14. Every subspace of dimension 1 in $\mathbb{F}_p^2$ is subgroup of $\mathbb{F}_p^2$, but it is not characteristic because it is not stable under $\mathrm{Aut}(\mathbb{F}_p^2) = \mathrm{GL}_2(\mathbb{F}_p)$.

3.3 Semidirect Products

Let N be a normal subgroup of G. Each element g of G defines an automorphism of N, $n \mapsto gng^{-1}$, and this defines a homomorphism

$$\theta : G \to \mathrm{Aut}(N), \quad g \mapsto i_g|_N .$$

If there exists a subgroup Q of G such that $G \to G/N$ maps Q isomorphiscally onto G/N, then we can reconstruct G from N, Q, and the restriction of θ to Q. Indeed, an element g of G can be written uniquely in the form

$$g = nq, \quad n \in N, \quad q \in Q,$$

since any element $g \in G$ falls in a unique coset of N. q must be the unique element of Q mapping to $gN \in G/N$, and n must be gq^{-1}. Thus, we have a one-to-one correspondence of sets

$$G \xleftrightarrow{1:1} N \times Q.$$

If $g = nq$ and $g' = n'q'$, then

$$gg' = (nq)(n'q') = n(qn'q^{-1})qq' = n \cdot \theta(q)(n') \cdot qq'.$$

Definition 3.15. A group G is a *semidirect product* of its subgroups N and Q if N is normal and the homomorphism $G \to G/N$ induces an isomorphism $Q \to G/N$. Equivalently, G is a semidirect product of subgroup N and Q if

$$N \triangleleft G; \quad NQ = G; \quad N \cap Q = \{1\} .$$

When G is the semidirect product of subgroups N and Q, we write $G = N \rtimes Q$(or $N \rtimes_\theta Q$, where $\theta : Q \to \mathrm{Aut}(N)$).

Example 3.16. In D_n, $n \geq 2$, let $C_n = \langle r \rangle$ and $C_2 = \langle s \rangle$; then

$$D_n = \langle r \rangle \rtimes_\theta \langle s \rangle = C_n \rtimes C_2,$$

where $\theta(s)(r^i) = r^{-i}$.

Example 3.17. The alternating subgroup A_n is a normal subgroup of S_n and $C_2 = \langle (12) \rangle$ maps isomorphically onto S_n/A_n. Therefore $S_n = A_n \rtimes C_2$.

Example 3.18. Let $G = \mathrm{GL}_n(F)$. Let B be the subgroup of upper triangular matrices in G, T the subgroup of diagonal matrices in G, and U the subgroup of upper triangular matrices with all their diagonal coefficients equal to 1. When $n = 2$, U is a normal subgroup of B, $UT = B$, and $U \cap T = \{1\}$. Therefore,

$$B = U \rtimes T.$$

Note that, when $n \geq 2$, the action of T on U is not trivial, for example

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{pmatrix} = \begin{pmatrix} 1 & ac/b \\ 0 & 1 \end{pmatrix},$$

and so B is not the direct product of T and U.

Example 3.19. 1. The quaternion group can not be written as a semidirect product in any nontrivial fashion.

2. A cyclic group of order p^2, p prime, is not a semidirect product, because it has only one subgroup of order p.

We have seen that, from a semidirect product $G = N \rtimes Q$, we obtain a triple

$$(N, Q, \theta : Q \to \mathrm{Aut}(N)),$$

and that the triple determines G.

Proposition 3.20. *Every triple (N, Q, θ) consisting of two groups N and Q and a homomorphism $\theta : Q \to \mathrm{Aut}(N)$. As a set, let $G = N \times Q$, and define*

$$(n, q)(n', q') = (n \cdot \theta(q)(n'), qq').$$

Then G is a group, and, in fact, the semidirect product of N and Q.

Proof. Write ${}^q n$ for $\theta(q)(n)$, so that the composition law becomes

$$(n, q)(n', q') = (n \cdot {}^q n', qq').$$

Then

$$((n, q), (n', q'))(n'', q'') = (n \cdot {}^q n' \cdot {}^{qq'} n'', qq'q'') = (n, q)((n', q')(n'', q''))$$

and so the asscociative law holds. Because $\theta(1) = 1$ and $\theta(q)(1) = 1$,

$$(1, 1)(n, q) = (n, q) = (n, q)(1, 1),$$

and so $(1, 1)$ is an identity element. Next

$$(n, q)({}^{q^{-1}} n^{-1}, q^{-1}) = (1, 1)({}^{q^{-1}} n^{-1}, q^{-1})(n, q),$$

and so $({}^{q^{-1}} n^{-1}, q^{-1})$ is an inverse for (n, q). Thus G is a group, and it is obvious that $N \lhd G, NQ = G$ and $N \cap Q = \{1\}$ and so $G = N \rtimes Q$. □

Example 3.21. A *group of order* 12. Let θ be the nontrivial homomorphism

$$C_4 \to \mathrm{Aut}(C_3) \simeq C_2,$$

namely, that sending a generator of C_4 to the map $a \mapsto a^2$. Then $G := C_3 \rtimes_\theta C_4$ is a noncommutative group of order 12, not isomorphic to A_4. If we denote the generators of C_3 and C_4 by a and b, then a and b generatate G, and have the defining relations

$$a^3 = 1, \quad b^4 = 1, \quad bab^{-1} = a^2.$$

Example 3.22. *Making outer automorphisms inner.* Let α be an automorphism, possibly outer, of a group N. We can realize N as a normal subgroup of a group G in such a way that α becomes the restriction to N of an inner automorphism of G. To see this, let $\theta : C_\infty \to \mathrm{Aut}(N)$ be the homomorphism sending a generator a of C_∞ to $\alpha \in \mathrm{Aut}(N)$, and let $G = N \rtimes_\theta C_\infty$. The element $g = (1, a)$ of G has the property that $g(n, 1)g^{-1} = (\alpha(n), 1)$ for all $n \in N$.

It will be useful to have criteria for when two triples (N, Q, θ) and (N, Q, θ') determine isomorphic groups.

Lemma 3.23. *If there exists an $\alpha \in \mathrm{Aut}(N)$ such that*

$$\theta'(q) = \alpha \circ \theta(q) \circ \alpha^{-1}, \quad \text{all } q \in Q,$$

then the map

$$\gamma : (n, q) \mapsto (\alpha(n), q) \quad N \rtimes_\theta Q \to N \rtimes_{\theta'} Q$$

is an isomorphism.

Proof. For $(n, q) \in N \rtimes_\theta Q$, then

$$\begin{aligned}\gamma(n, q) \cdot \gamma(n', q') &= (\alpha(n), q) \cdot (\alpha(n'), q') \\ &= (\alpha(n) \cdot (\alpha \circ \theta(q) \circ \alpha^{-1})(\alpha(n')), qq') \\ &= (\alpha(n) \cdot \alpha(\theta(q)(n')), qq'),\end{aligned}$$

and

$$\begin{aligned}\gamma((n, q) \cdot (n', q')) &= \gamma(n \cdot \theta(q)(n'), qq') \\ &= (\alpha(n) \cdot \alpha(n) \cdot \alpha(\theta(q)(n')), qq').\end{aligned}$$

Therefore γ is a homomorphism. The map

$$(n, q) \mapsto (\alpha^{-1}(n, q)) : \quad N \rtimes_{\theta'} Q \to N \rtimes_\theta Q$$

is also a homomorphism, and it is inverse to γ. □

Lemma 3.24. *If $\theta = \theta' \circ \alpha$ with $\alpha \in \mathrm{Aut}(Q)$, then the map*

$$\gamma : (n, q) \mapsto (n, \alpha(q)) \quad N \rtimes_\theta Q \simeq N \rtimes_{\theta'} Q$$

is an isomorphism.

Proof.

$$\begin{aligned}\gamma(n, q) \cdot \gamma(n', q') &= (n, \alpha(q))(n', \alpha(q')) \\ &= (n \cdot \theta' \circ \alpha(q)(n'), \alpha(qq')) \\ &= (n \cdot \theta(q)n, \alpha(qq')) \\ &= \gamma(n \cdot \theta(q)(n'), qq') = \gamma((n, q) \cdot (n', q')).\end{aligned}$$

□

Lemma 3.25. *If Q is finite and cyclic and the subgroup $\theta(G)$ of $\mathrm{Aut}(N)$ is conjugate to $\theta'(Q)$, then*

$$N \rtimes_\theta Q \simeq N \rtimes_{\theta'} Q.$$

Proof. Let a generate Q. By assumption, there exists an $\alpha' \in Q$ and an $\alpha \in \mathrm{Aut}(N)$ such that

$$\theta'(a') = \alpha \cdot \theta(a) \cdot \alpha^{-1}.$$

The element $\theta'(a')$ generatates $\theta'(Q)$, and we can choose a' to generate Q, say $a' = a^i$. Now the map $(n, q) \mapsto (\alpha(n), q^i)$ is an isomorphism $N \rtimes_\theta Q \to N \rtimes_{\theta'} Q$, with the inverse $(n, q^i) \mapsto (\alpha^{-1}(n), q)$. □

Theorem 3.26. *Let G be a group with subgroups H_1 and H_2 such that $G = H_1 H_2$ and $H_1 \cap H_2 = \{e\}$, so that each element g of G can be writtern uniquely as $g = h_1 h_2$ with $h_1 \in H_1$ and $h_2 \in H_2$.*

1. *If H_1 and H_2 are both normal, then G is the direct product of H_1 and H_2, $G = H_1 \times H_2$.*
2. *If H_1 is normal in G, then G is the semidirect product of H_1 and H_2, $G = H_1 \rtimes H_2$.*
3. *If neither H_1 nor H_2 is normal, then G is the Zappa-Szép (or knit) product of H_1 and H_2.*

3.4 Extensions of Groups

Definition 3.27. A group G is *complete* if the map $g \mapsto i_g : G \to \mathrm{Aut}(G)$ is an isomorphism.

Proposition 3.28. *A group G is a complete if and only if*

1. *the centre $Z(G)$ of G is trivial.*
2. *every automorphism of G is inner.*

Example 3.29. The group S_n is complete for $n \neq 2, 6$, but S_2 fails (1) and S_6 fails (2) in the preceding proposition.

Example 3.30. If G is a simple noncommutative group, then $\mathrm{Aut}(G)$ is complete.

Definition 3.31. A sequence of groups and homomorphisms

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} 1 \tag{2}$$

is *exact* if ι is injective, π is surjective, and $\ker \pi = \mathrm{Im}(\iota)$.

Thus $\iota(N)$ is a normal subgroup of G and $G/\iota(N) \simeq Q$. We often identify N with the subgroup $\iota(N)$ of G and Q with the quotient G/N.

Definition 3.32. An exact sequence 2 is also called an *extension of* Q by N. An extension is *central* if $\iota(N) \subseteq Z(G)$.

For example, a semidirect product $N \rtimes_\theta Q$ gives rise to an extension of Q by N,

$$1 \to N \to N \rtimes_\theta Q \to Q \to 1,$$

which is central $\iff$ θ is the trivial homomorphism and N is commutative:

$$(n, q)(n', 1)({}^{q^{-1}}n^{-1}, q^{-1}) = (n, q)(n' \cdot {}^{q^{-1}}n^{-1}, q^{-1}) = (n \cdot {}^{q}(n' \cdot {}^{q^{-1}}n^{-1}), 1)$$

Definition 3.33. Two extensions of Q by N are said to be *isomorphic* if there exists a commutative diagram

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] \arrow[d, equal] & G \arrow[r] \arrow[d, dashed, "\simeq"] & Q \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & N \arrow[r] & G' \arrow[r] & Q \arrow[r] & 1 \end{tikzcd}$$

Definition 3.34. An extension of Q by N,

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1,$$

is said to be *split* if it is isomorphic to the extension definded by a semidirect product $N \rtimes_\theta Q$.

Remark 3.35. Equivalent conditions:

1. there exists a subgroup $Q' \subseteq G$ such that π induces an isomorphism $Q' \to Q$;
2. there exists a homomorphism: $s : Q \to G$ such that $\pi \circ s = \mathrm{id}.(G = \iota(N) \rtimes s(Q))$.

In general, an extension will not split.

Example 3.36. For example,

$$1 \to C_p \to C_{p^2} \to C_p \to 1$$

doesn't split. If Q is the quaternion group and N is its centre, then

$$1 \to N \to Q \to Q/N \to 1$$

doesn't split.(if it did, Q would be commutative because N and Q/N are commutative and θ trivial(N is its centre))

Theorem 3.37 (Schur-Zassenhaus)**.** *An extension of finite groups of relatively prime order is split.*

Proposition 3.38. *An extension 2 splits if N is complete. In fact, G is then the direct product of N with the* centralizer *of N in G,*

$$C_G(N) := \{g \in G : gn = ng \text{ all } n \in N\}.$$

Proof. Let $H = C_G(N)$.

1. for any $g \in G, n \mapsto gng^{-1} : N \to N$ is an automorphism of N(N is already a normal subgroup of G), and it must be the inner automorphism defined by an element γ of N; thus

$$gng^{-1} = \gamma n \gamma^{-1} \quad \text{all } n \in N.$$

   It implies that $\gamma^{-1}g \in H$, and hence $g = \gamma(\gamma^{-1}g) \in NH$. Since g is arbitrary, $G = NH$.

2. N is complete and hence $Z(N) = \{e\}$.

3. Finally, for any element $g = nh \in G$,

$$gHg^{-1} = n(hHh^{-1})n^{-1} = nHn^{-1} = H$$

   Therefore, H is normal in G. Hence, $G = N \times H$ by 1.51.

□

4 Groups Acting on Sets

4.1 Actions

Definition 4.1. Let X be a set and let G be a group. A *left action* of G on X is a mapping $(g, x) \mapsto gx : G \times X \to X$ such that

1. $1x = x$, for all $x \in X$;
2. $(g_1g_2)x = g_1(g_2x)$, all $g_1, g_2 \in G, x \in X$.

A set together with a left action of G is called a (left) *G-set*. An action is *trivial* if $gx = x$ for all $g \in G$.

The conditions imply that, for each $g \in G$, left translation by g,

$$g_L : X \to X, \quad x \mapsto gx,$$

has $(g^{-1})_L$ as an inverse, and therefore g_L is a bijection, i.e. $g_L \in \mathrm{Sym}(X)$. (2) now says that

$$g \mapsto g_L : G \to \mathrm{Sym}(X)$$

is a homomorphism.

Definition 4.2. The action is said to be *faithful*(or *effective*) if the homomorphism is injective, i.e., if

$$gx = x \text{ for all } x \in X \implies g = 1.$$

Example 4.3. Every subgroup of the symmetric group S_n acts faithfully on $\{1, 2, \cdots, n\}$.

Example 4.4. Every subgroup H of a group G acts faithfully on G by left translation,

$$H \times G \to G, \quad (h, x) \mapsto hx.$$

Example 4.5. The *group of rigid motions* of $\mathbb{R}^n$ is the group ob bijections $\mathbb{R}^n \to \mathbb{R}^n$ preserving lengths.

Definition 4.6. A *G-map of G*-sets is a map $\varphi : X \to Y$ such that

$$\varphi(gx) = g\varphi(x), \quad \text{all } g \in X, \quad x \in X.$$

An *isomorphism* of G-sets is a bijective G-maps; its inverse is then also a G-map.

Definition 4.7. Let G act on X. A subset $S \subseteq X$ is said to be *stable* under the action of G if

$$g \in G, x \in S \implies gx \in S.$$

The action of G on X then induces an action of G on S. Write $x \sim_G y$ if $y = gx$, for some $g \in G$. This is an equivalence relation. The equivalence classes are called *G-orbits*. Thus the G-orbits partition X. Write $G \backslash X$ for the set of orbits.

Remark 4.8. By definition, the G-orbit containing x_0 is

$$Gx_0 = \{gx_0 : g \in G\}.$$

It is the smallest G-stable subset of X containing x_0. And a subset of X is stable $\iff$ it is a union of orbits.

Example 4.9. Suppose G acts on X, and let $\alpha \in G$ be an element of order n. Then the orbits of $\langle \alpha \rangle$ are the sets of the form

$$\left\{x_0, \alpha x_0, \cdots, \alpha^{n-1} x_0\right\}.$$

And these elements need not be distinct.

Definition 4.10. The action of G on X is said to be *transitive*, and G is said to act *trasitively* on X, if there is only one orbit. The set X is then called a *homogeneous* G-set.

Example 4.11. S_n acts transitively on $\{1, 2, \cdots, n\}$.

Example 4.12. For any subgroup H of a group G, G acts transitively on G/H. But the action of G on itself by conjugation is never transitive if $G \neq 1$, because $\{1\}$ is always a conjugacy class.

Definition 4.13. The action of G on X is *doubly transitive* if for any two pairs $(x_1, x_2), (y_1, y_2)$ of elements of X with $x_1 \neq x_2$ and $y_1 \neq y_2$, there exists a single $g \in G$ such that $gx_1 = y_1$ and $gx_2 = y_2$. Define *k-fold transitivity* for $k \geq 3$ similarly.

Definition 4.14. Let G act on X. The *stabilizer* (or *isotropy group*) of an element $x \in X$ is

$$\operatorname{Stab}(x) = \{g \in G : gx = x\}.$$

The action is *free* if $\operatorname{Stab}(x) = \{e\}$ for all x.

$\operatorname{Stab}(x)$ is a subgroup, but it need not be a normal subgroup, and more precisely, we have the following

Lemma 4.15. *For any $g \in G$ and $x \in X$,*

$$\operatorname{Stab}(gx) = g \cdot \operatorname{Stab}(x) \cdot g^{-1}.$$

Definition 4.16. Let G act on itself by conjugation. Then

$$\operatorname{Stab}(x) = \{g \in G : gx = xg\}.$$

This group is called the *centralizer* $C_G(x)$ of x in G. It consists of all elements of G that commute with, i.e., centralize, x. The intersection

$$\bigcap_{x \in G} C_G(x) = \{g \in G : gx = xg \text{ for all } x \in G\}$$

is the centre of G.

Example 4.17. Let G act on G/H by left multiplication. Then $\operatorname{Stab}(H) = H$ and the stabilizer of gH is gHg^{-1}.

Definition 4.18. For a subset S of X, we define the *stabilizer* of S to be

$$\operatorname{Stab}(S) = \{g \in G : gS = S\}.$$

Like 4.15, We also have

$$\mathrm{Stab}(gS) = g \cdot \mathrm{Stab}(S) \cdot g^{-1}.$$

Definition 4.19. Let G act on G by conjugation, and let H be a subgroup of G. The stabilizer of H is called the *normalizer* $N_G(H)$ of H in G:

$$N_G(H) = \left\{ g \in G : gHg^{-1} = H \right\}.$$

$N_G(H)$ is the largest subgroup of G containing H as a normal subgroup.

Proposition 4.20. *If G acts transitively on X, then for any $x_0 \in X$, the map*

$$g \,\mathrm{Stab}(x_0) \mapsto gx_0 : G/\,\mathrm{Stab}(x_0) \to X$$

is an isomorphism of G-sets.

Corollary 4.21. *Let G act on X, and let $O = Gx_0$ be the orbit containing x_0. Then the cardinality of O is*

$$|O| = (G : \mathrm{Stab}(x_0)).$$

Proposition 4.22. *Let $x_0 \in X$. If G acts transitively on X, then*

$$\ker(G \to \mathrm{Sym}(X))$$

is the largest normal subgroup contained in $\mathrm{Stab}(x_0)$.

Proof. It follows from the equation below and 1.33.

$$\ker(G \to \mathrm{Sym}(X)) = \bigcap_{x \in X} \mathrm{Stab}(x) = \bigcap_{g \in G} \mathrm{Stab}(gx_0) = \bigcap g \cdot \mathrm{Stab}(x_0) \cdot g^{-1}.$$

□

When X is finite, it is a disjoint union of a finite number of orbits

$$X = \bigcup_{i=1}^{m} O_i$$

Hence by 4.21, we have the following results

Proposition 4.23. *The number of elements in X is*

$$|X| = \sum_{i=1}^{m} |O_i| = \sum_{i=1}^{m} (G : \mathrm{Stab}(x_i)), \quad x_i \in O_i.$$

Proposition 4.24 (Class Equation)**.**

$$|G| = \sum (G : C_G(x))$$

where x runs over a set of representatives for the conjugacy classes, or

$$|G| = |Z(G)| + \sum (G : C_G(y))$$

where y runs over set of representatives for the conjugacy classes containing more than one element.

Theorem 4.25 (Cauchy)**.** *If the prime p divides $|G|$, then G contains an element of order p.*

Proof. We use induction on $|G|$. If for some y not in the centre of G and p does not divide $(G : C_G(y))$. Then p divides the order of $C_G(y)$ and we apply induction. Thus we may suppose that p divides all of the terms $(G : C_G(y))$ in the class equation, and also divides $Z(G)$. But $Z(G)$ is commutative, and follows from the structure theorem of such groups that $Z(G)$ will contain an element of order p. □

Corollary 4.26. *A finite group G is a p-group if and only if every element has order a power of p.*

Proof. "only if" part follows from Lagrange's theorem 1.18. "if" part follows from Cauchy's theorem 4.25: if not, suppose another $p \neq p' \mid |G|$, then there exists an element $a \in G$ with order p' contained in G, a contradiction. $\square$

Corollary 4.27. *Every group of order $2p$, where p is odd prime, is cyclic or dihedral.*

Proof. From Cauchy's theorem 4.25, we know that such a group G contains elements s and r of orders 2 and p respectively. Then H with index 2 is normal. Obviously, $s \notin H$, and so $G = H \cup Hs$:

$$G = \left\{1, r, \cdots, r^{p-1}, s, rs, \cdots, r^{p-1}s\right\}.$$

As H is normal, $srs^{-1} = r^i$ for some i. Because $s^2 = 1, r = s^2rs^{-2} = s(srs^{-1})s^{-1} = r^{i^2}$, and so $i^2 \equiv 1 \mod p$. Because $\mathbb{Z}/p\mathbb{Z}$ is a field, its only elements with square 1 are ± 1, and so $i \equiv 1$ or $-1 \mod p$. In the first case, the group is commutative; in the second $srs^{-1} = r^{-1}$ and so it is the dihedral group. $\square$

Theorem 4.28. *Every nontrivial finite p-group has nontrivial centre.*

Proof. 4.24 $\square$

Corollary 4.29. *A group of order p^n has normal subgroups of order p^m for all $m \leq n$.*

Proof. We use induction on n. Let G be a group with order p^n. By Cauchy'theorem 4.25, $Z(G)$ contains an element g of order p, and so $N = \langle g \rangle$ is a normal subgroup of G of order p. It follows from the induction hypothesis to G/N and 1.47. $\square$

Proposition 4.30. *Every group of order p^2 is commutative, and hence is isomophic to $C_p \times C_p$ or C_{p^2}.*

Proof. 4.31 $\square$

Lemma 4.31. *Suppose G contains a subgroup H in its centre(hence H is normal) such that G/H is cyclic. Then G is commutative.*

Proof. Let a be an element of G whose image in G/H generates *it*. Then every element of G can be written $g = a^ih$ with $h \in H, i \in \mathbb{Z}$. Now

$$a^ih \cdot a^{i'}h' = a^{i'}h' \cdot a^ih,$$

by using the fact that $H \subseteq Z(G)$. $\square$

4.2 Permutation Groups

Definition 4.32. Consider $\mathrm{Sym}(X)$, where X has n elements and consider a permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

The ordered pairs (i, j) with $i < j$ and $\sigma(i) > \sigma(j)$ are called the *inversions* of σ, and σ is said to be *even* or *odd* according as the number its inversions is even or odd. The *signature*, $\mathrm{sign}(\sigma)$, of σ is $+1$ or -1 according as σ is even or odd.

Proposition 4.33. $\mathrm{sign}(\sigma)\,\mathrm{sign}(\tau) = \mathrm{sign}(\sigma\tau)$.

Proof. For a permutation σ, consider the products

$$V = \prod_{1 \leq i < j \leq n} (j - i) = (2-1)(3-1)\cdots(n-1)(3-2)\cdots(n-2)\cdots(n-(n-1))$$

and

$$\sigma V = \prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)).$$

Both products run over the 2-element subsets $\{i,j\}$ of $\{1,2,\cdots,n\}$ and the terms correponding to a subset are the same except that each inversion introduces a negative sgin. Therefore,

$$\sigma V = \mathrm{sign}(\sigma)(V).$$

Now let P be the additive group of maps $\mathbb{Z}^n \to \mathbb{Z}$. For $f \in P$ and $\sigma \in S_n$, let σf denote the element of P defined by

$$(\sigma f)(z_1,\cdots,z_n) = f(z_{\sigma(1)},\cdots,z_{\sigma(n)}).$$

For $z \in \mathbb{Z}^n$ and $\sigma \in S_n$, let z^σ denote the element of $\mathbb{Z}^n$ such that $(z^\sigma)_i = z_{\sigma(i)}$. Then $(z^\sigma)^\tau = z^{\sigma\tau}$. By definition, we have

$$\sigma(\tau f) = (\sigma\tau)f.$$

Let p be the element of P defined by

$$p(z_1,\cdots,z_n) = \prod_{1\le i<j\le n}(z_j - z_i).$$

Then

$$\sigma p = \mathrm{sign}(\sigma)p.$$

□

Definition 4.34. In 4.33, we show that sign is a homomorphism $S_n \to \{\pm 1\}$. When $n \geq 2$, it is surjective, and so its kernel is a normal subgroup of S_n or order $n!/2$, called the *alternating group* A_n.

Definition 4.35. A *cycle* is a permutation of the following form

$$i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_r \mapsto i_1, \quad \text{remaining } i\text{'s fixed.}$$

The i_j are required to be distinct. We denote this cycle by $(i_1 i_2 \cdots i_r)$, and call r its *length.* A cycle of length 2 is a *transposition.* A cycle of length 1 is the identity map. The *support of the cycle* $(i_1 \cdots i_r)$ is the set $\{i_1,\cdots,i_r\}$, and cycles are said to be *disjoint* if their supports are disjoint.

Remark 4.36. Disjoint cycles commute. And if

$$\sigma = (i_1\cdots i_r)(j_1\cdots j_s)\cdots(l_1\cdots l_u)$$

then

$$\sigma^m = (i_1\cdots i_r)^m(j_1\cdots j_s)^m\cdots(l_1\cdots l_u)^m$$

and it follows that σ has order $\mathrm{lcm}(r,s,\cdots,u)$.

Proposition 4.37. *Every permutation can be written as a product of disjoint cycles.*

Example 4.38.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 4 & 2 & 1 & 3 & 6 & 8 \end{pmatrix} = (15)(27634)(8).$$

Corollary 4.39. *Each permutation σ can be written as a product of transpositions; the number of transpositions in such a product is even or odd according as σ is even or odd. In particular, the signature of a cycle of length r is $(-1)^{r-1}$, that is, an r-cycle is even or odd according as r is odd or even.*

Proof. Noting that $(i_1 i_2\cdots i_r) = (i_1 i_2)\cdots(i_{r-2}i_{r-1})(i_{r-1}i_r)$. □

Corollary 4.40. *The alternating group A_n is generated by cycles of length three.*

Proof.

$$(ij)(kl) = \begin{cases} (ij)(jl) = (ijl) & j = k, \\ (ij)(jk)(jk)(kl) = (ijk)(jkl) & i,j,k,l \text{ distinct} \\ 1 & (ij) = (kl) \end{cases}$$

□

In S_n, the conjugate of a cycle is given by

$$g(i_1 \cdots i_k)g^{-1} = (g(i_1) \cdots g(i_k)).$$

We shall determine the conjugacy classes in S_n.

Definition 4.41. By a *partition* of n, we mean a sequence of integers $n_1, \cdots, n_k$ such that

$$1 \leq n_1 \leq n_2 \leq \cdots n_k \leq n \text{ and } n_1 + n_2 + \cdots + n_k = n.$$

Proposition 4.42. *Two elements σ and τ of S_n are conjugate if and only if they define the same partitions of n.*

Proof. $\Longleftarrow$: Since σ and τ define the same partitions of n, their decompositions into products of disjoint cycles have the same type:

$$\sigma = (i_1 \cdots i_r)(j_1 \cdots j_s) \cdots (l_1 \cdots l_u),$$
$$\tau = (i'_1 \cdots i'_r)(j'_1 \cdots j'_s) \cdots (l'_1 \cdots l'_u).$$

If we define g to be

$$\begin{pmatrix} i_1 & \cdots & i_r & j_1 & \cdots & j_s & \cdots & l_1 & \cdots & l_u \\ i'_1 & \cdots & i'_r & j'_1 & \cdots & j'_s & \cdots & l'_1 & \cdots & l'_u \end{pmatrix}$$

□

Remark 4.43. For $1 < k \leq n$, there are $\frac{n(n-1)\cdots(n-k+1)}{k}$ distinct k-cycles in S_n. The $1/k$ is needed so that we don't count

$$(i_1 i_2 \cdots i_k) = (i_k i_1 \cdots i_{k-1}) = \cdots$$

k times. Similarly, it is possible to compute the number of elements in any conjugacy class in S_n, but a little care is needed when the partition of n has several terms equal. For example, the number of permutation in S_4 of type $(ab)(cd)$ is

$$\frac{1}{2}\left(\frac{4 \cdot 3}{2} \cdot \frac{2 \cdot 1}{2}\right) = 3.$$

The $\frac{1}{2}$ is needed so that we don't count $(ab)(cd) = (cd)(ab)$ twice. For S_4 we have the follow table:

partition	element	No. in Conj. Class	Parity
$1+1+1+1$	1	1	even
$1+1+2$	(ab)	6	odd
$1+3$	(abc)	8	even
$2+2$	$(ab)(cd)$	3	even
4	$(abcd)$	6	odd

Note that A_4 contains exactly 3 elements of order 2, namely those of type $2+2$, and that with 1 they form a subgroup V. This group is a union of conjugacy classes, and is therefore a normal subgroup of S_4.

Theorem 4.44 (Galois)**.** *The group A_n is simple if $n \geq 5$.*

Proof. 4.46 and 3.8. □

Remark 4.45. For $n = 2$, A_n is trivial, and for $n = 3$, A_n is cyclic of order 3, and hence simple.

Lemma 4.46. *Let N be a normal subgroup of $A_n (n \geq 5)$; if N contains a cycle of length three, then it contains all cycles of length three, and so equal A_n.*

Proof. Let γ be the cycle of length three in N, and let σ be a second cycle of length three in A_n. We know that $\sigma = g\gamma g^{-1}$ for some $g \in S_n$.

- If $g \in A_n$, then this shows that σ is also in N.

- If not, because $n \geq 5$, there exists a transposition $t \in S_n$ disjoint from σ. Then $tg \in A_n$, and
$$\sigma = t\sigma t^{-1} = tg\gamma g^{-1} t^{-1},$$
and so again $\sigma \in N$.

□

Lemma 4.47. *Every normal subgroup N of A_n, $n \geq 5$, $N \neq 1$, contains a cycle of length 3.*

Proof. Let $\sigma \in N$, $\sigma \neq 1$. If σ is not a 3-cycle, then $\sigma' \neq 1$, which fixes more elements of $\{1, 2, \cdots, n\}$ than does σ. If σ' is not, we can apply the same construction. After a finite number of steps, we arrive at a 3-cycle.

Suppose σ is not a 3-cycle. When we express it as a product of disjoint cycles, either it contains a cycle of length ≥ 3 or else it is a product of transpositions.

1. $\sigma = (i_1 i_2 i_3 \cdots) \cdots$. σ moves two numbers, say i_4, i_5 other than i_1, i_2, i_3 since $\sigma \neq (i_1 i_2 i_3), (i_1 \cdots i_4)$. Let $\gamma = (i_3 i_4 i_5)$, then $\sigma_1 := \gamma\sigma\gamma^{-1} = (i_1 i_2 i_4 \cdots) \cdots \in N$, and is distinct from σ. Thus $\sigma' := \sigma_1 \sigma^{-1} \neq 1$, but $\sigma' = \gamma\sigma\gamma^{-1}\sigma^{-1}$ fixes i_2 and all elements other than $i_1, \cdots, i_5$ fixed by σ. Therefore, it fixes more elements than σ.

2. $\sigma = (i_1 i_2)(i_3 i_4) \cdots$. form $\gamma, \sigma_1, \sigma'$ as the first case with i_4 as in (2) and i_5 any element distinct from i_1, i_2, i_3, i_4. Then $\sigma_1 = (i_1 i_2)(i_4 i_5) \cdots$ is distinct from σ because it acts differently on i_4. Thus $\sigma' = \sigma_1 \sigma^{-1} \neq 1$, but σ' fixes i_1 and i_2, and all elements $\neq i_1, \cdots, i_5$ not fixed by σ. Therefore it fixes at least one more element than σ.

□

Corollary 4.48. *For $n \geq 5$, the only normal subgroups of S_n are 1, A_n, and S_n.*

Proof. If N is normal in S_n, then either $N \cap A_n = A_n$ or $N \cap A_n = \{1\}$. In the second case, the map $x \mapsto xA_n : N \to S_n/A_n$ is injective, but it can't have order 2 because no conjugacy class in S_n consists of a single element. □

4.3 The Todd-Coxeter algorithm

Let G be a group described by a finite presentation, and let H be a subgroup described by a generated set. Then the *Todd-Coxeter algorithm* is a strategy for writing down the set of left cosets of H in G together with the action of G on the set.

Let $G = \langle a, b, c \mid a^3, b^2, c^2, cba \rangle$ and let H be the subgroup generated by c. The operation of G on the set of cosets is described by the action of generators which must satisfy the following rules

1. Each generator acts as a permutation.

2. The relations act trivially.

3. The generators of H fix the coset $1H$.

4. The operation on the cosets is transitive.

4.4 Primitive actions

Definition 4.49. Let G be a group acting on a set X, and let π be a partition of X. We say that π is *stabilized* by G if
$$A \in \pi \implies gA \in \pi.$$

Example 4.50. 1. The subgroup $G = \langle (1234) \rangle$ of S_4 stabilizes the partition $\{\{1, 3\}, \{2, 4\}\}$ of $\{1, 2, 3, 4\}$.

2. Identify $X = \{1, 2, 3, 4\}$ with the set of vertices of the square on which D_4 acts in the usual way, namely, with $r = (1234)$, $s = (24)$. Then D_4 stabilizes the partition $\{\{1, 3\}, \{2, 4\}\}$(opposite vertices stay opposite).

Definition 4.51. The group G always stabilizes the trivial partitions of X, namely, the set of all one-element subsets of X, and $\{X\}$. When it stabilizes only those partitions, we say that the action is *primitive*; otherwise it is *imprimitive.* A subgroup of $\mathrm{Sym}(X)$ is said to be *primitive* if it acts primitively on X.

Example 4.52. S_n itself is primitive.

Example 4.53. A doubly transitive action is primitive: if it stabilized

$$\{\{x, x'\}, \{y, \cdots, \}, \cdots\},$$

then there would be no element sending (x, x') to (x, y).

Proposition 4.54. *Let G be a finite group acting transitively on a set X with at least two elements. The group G acts imprimitively $\iff$ there is a proper subset A of X with at least 2 elements such that*

$$\text{for each } g \in G, \text{ either } gA = A \text{ or } gA \cap A = \emptyset. \tag{3}$$

Proof. $\Longleftarrow$: From such an A, we can form a partition $\{A, g_1A, g_2A, \cdots\}$ of X, which is stabilized by G(Recall that we assume G acts transitively on X). □

Definition 4.55. Let G be a finite group acting transitively on a set X with at least two elements. A subset A of X satisfying 3 is called *block.*

Lemma 4.56. *Let G be a finite group acting transitively on a set X with at least two elements. Let A be a block in X with $|A| \geq 2$ and $A \neq X$. For any $x \in A$,*

$$\mathrm{Stab}(x) \subsetneq \mathrm{Stab}(A) \subsetneq G.$$

Proof. $\mathrm{Stab}(A) \supseteq \mathrm{Stab}(x)$ because

$$gx = x \implies gA \cap A \neq \emptyset \implies gA = A.$$

Let $y \in A, y \neq x$. Because G acts transitively on X, there is a $g \in G$ such that $gx = y$. Then $g \in \mathrm{Stab}(A)$, but $g \notin \mathrm{Stab}(x)$. Let $y \notin A$. There is a $g \in G$ such that $gx = y$, and then $g \notin \mathrm{Stab}(x)$. □

Theorem 4.57. *Let G be a finite group acting transitively on a set X with at least two elements. The group G acts primitively on X $\iff$ for one $x \in X, \mathrm{Stab}(x)$ is a maximal subgroup(hence any) of G.*

Proof. $\Longleftarrow$ follows from 4.56. $\Longrightarrow$: suppose that there exists an x in X and a subgroup H such that

$$\mathrm{Stab}(x) \subsetneq H \subsetneq G.$$

Then we claim that $A = Hx$ is a block $\neq X$ with at least two elements. Because $H \neq \mathrm{Stab}(x), Hx \neq \{x\}$, and so $\{x\} \subsetneq A \subsetneq X$. If $g \in H$, then $gA = A$. If $g \notin H$, then gA is disjoint from A: for suppose $ghx = h'x$ for some $h' \in H$; then $h'^{-1}gh \in \mathrm{Stab}(x) \subseteq H$, say $h'^{-1}gh = h''$, and $g = h'h''h^{-1} \in H$. □

4.5 Sylow Theorem

In this subsection, all group are finite.

Definition 4.58. Let G be a group and let p be a prime dividing $(G : 1)$. A subgroup of G is called a *Sylow p-subgroup of G* if its order is the highest power of p dividing $(G : 1)$.

In the proofs, we frequently use that if O is an orbit for a group H acting on a set X, and $x_0 \in O$, then the map $H \to X, h \mapsto hx_0$ induces a bijection

$$H/\mathrm{Stab}(x_0) \to O;$$

Therefore

$$(H : \mathrm{Stab}(x_0)) = |O|.$$

In particular, when H is a p-group, $|O|$ is a power of p, and so either O consists of a single element, or $|O|$ is divisible by p.

Theorem 4.59 (Sylow I)**.** *Let G be a finite group, and let p be prime, then G has a subgroup of order p^r.*

Proof. It suffices to prove this with p^r the highest power of p dividing $(G:1)$, and so from now on we assume that $(G:1) = p^r m$ with $p \nmid m$. Let

$$X = \{\text{subsets of } G \text{ with } p^r \text{ elements}\},$$

with the action of G defined by

$$G \times X \to X, \quad (g, A) \mapsto gA.$$

Let $A \in X$, and let

$$H = \operatorname{Stab}(A) \coloneqq \{g \in G : gA = A\}.$$

For any $a_0 \in A, h \mapsto ha_0 : H \to A$ is injective, since $A \subseteq G$. And so $(H:1) \leq |A| = p^r$. In the equation

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

we know that $(G:1) = p^r m, (H:1) \leq p^r$ and that $(G:H)$ is the number of elements in the orbits of A. Observe that: if we can find an A such that p doesn't divide the number of elements in its orbit, then we can conclude that $H = \operatorname{Stab} A$ has order p^r. The number of elements in X is

$$|X| = \binom{p^r m}{p^r} = \frac{(p^r m)(p^r m - 1)\cdots(p^r m - i)\cdots(p^r m - p^r + 1)}{p^r(p^r - 1)\cdots(p^r - i)\cdots(p^r - p^r + 1)}.$$

Note that, because $i < p^r$, the power of p dividing $p^r m - i$ is the power of p dividing i. The same is true for $p^r - i$. Therefore the correponding terms on top and bottom are divisible by the same powers of p, and so p does not divide $|X|$. Because the orbits form a partition of X,

$$|X| = \sum |O_i|, \quad O_i \text{ the distinct orbits}.$$

and so at least one of the $|O_i|$ is not divisible by p. □

Lemma 4.60. *Let H be a p-group acting on a finite set X, and let X^H be the set of points fixed by H; then*

$$|X| \equiv \left|X^H\right| \pmod{p}.$$

Proof. 4.23. □

Lemma 4.61. *Let P be a Sylow p-subgroup of G, and let H be a p-subgroup. If H normalizes P, i.e., if $H \subseteq N_G(P)$, then $H \subseteq P$. In particular, no Sylow p-subgroup of G other than P normalizes P.*

Proof. Because H and P are subgroups of $N_G(P)$ with P normal in $N_G(P)$, HP is a subgroup, and $H/H \cap P \simeq HP/P$ Therefore $(HP:P)$ is a power of p, but

$$(HP:1) = (HP:P)(P:1),$$

and $(P:1)$ is the largest power of p dividing $(G:1)$, hence also the largest power of p dividing $(HP:1)$. Hence $(HP:P) = 1$, and $H \subseteq P$. □

Theorem 4.62 (Sylow II)**.** *Let G be a finite group, and let $|G| = p^r m$ with m not divisible by p.*

1. *Any two Sylow p-subgroups are conjugate.*
2. *Let s_p be the number of Sylow p-subgroups in G; then $s_p \equiv 1 \mod p$ and $s_p \mid m$.*
3. *Every p-subgroup of G is contained in a Sylow p-subgroup.*

Proof. 1. Let X be the set of Sylow p-subgroups in G, and let G ac on X by conjugation,

$$(g, P) \mapsto gPg^{-1}: \quad G \times X \to X.$$

Let O be one of the G-orbits: we have to show O is all of X.

Let $P \in O$, and let P act on O through the action of G. This single G-orbit may break up into serveral P-orbits, one of which will be $\{P\}$. In fact this is the only one-point orbit because

$$\{Q\} \text{ is a } P\text{-orbit} \iff P \text{ normalizes } Q.$$

We know that happens only for $Q = P$ by 4.61. Hence the number of elements in every P-orbit other than $\{P\}$ is divisible by p, and we have that $|O| \equiv 1 \mod p$.

Suppose there exists a $P \notin O$. We again let P act on O, but this time the argument shows that there are no one-point orbit, and so the number of elements in every P-orbit is divisible by p(the orbit equation). This implies that $\#O$ is divisible by p, which is a contradiction.

2. Let P be a Sylow p-subgroup of G. We have shown that $s_p \equiv 1 \pmod p$. Then

$$s_p = (G : N_G(P)) = \frac{(G:1)}{(N_G(P):1)} = \frac{(G:1)}{(N_G(P):P)\cdot(P:1)} = \frac{m}{(N_G(P):P)}.$$

3. Let H be a p-subgroup of G, and let H act on the set X of Sylow p-subgroups by conjugation. Because $|X| = s_p$ is not divisible by p, X^H must be nonemepty by 4.60. But then H normalizes P and the preceding lemma implies that $H \subseteq P$.

□

Corollary 4.63. *A Sylow p-subgroup is normal $\iff$ it is only Sylow p-subgroup.*

Corollary 4.64. *Suppose that a group G has only one Sylow p-subgroup for each prime p dividing its order. Then G is a direct product of its Sylow p-subgroups.*

Proof. Let $P_1, \cdots, P_k$ be Sylow subgroups of G, and let $|P_i| = p_i^{r_i}$, where the p_i are distinct primes. We shall prove by induction on k that it has order $p_1^{r_1}\cdots p_k^{r_k}$. We may suppose that $k \geq 2$ and $P_1 \cdots P_{k-1}$ has order $p_1^{r_1}\cdots p_{k-1}^{r_{k-1}}$. Then $P_1\cdots P_{k-1} \cap P_k = 1$ then $(P_1 \cdots P_{k-1})P_k$ is the direct product of $P_1 \cdots P_{k-1}$ and P_k, and so has order $p_1^{r_1}\cdots p_k^{r_k}$. □