Part 4: Special Topics

23 Sylow Theorems

23.1 Conjugacy Classes

Definition Conjugacy Class of a

> Let a and b be elements of a group G. We say that a and b are **conjugates** and call b a **conjugate** of a if $xax^{-1} = b$ for some x in G. The **conjugacy class** is the set $\mathrm{cl}(a) = \{xax^{-1} \mid x \in G\}$.

Theorem 23.1 Number of Conjugates of a

> Let G be a finite group and let a be an element of G, then $|\mathrm{cl}(a)| = |G : C(a)|$.

Proof $T : G/C(a) \to \mathrm{cl}(a),\ xC(a) \mapsto xax^{-1}$ is well-defined, one-to-one and onto.

- Similarly, $|\mathrm{cl}(H)| = |G : N(H)|$.

Corollary 1 $|\mathrm{cl}(a)|$ Divides $|G|$.

> In a finite group, $|\mathrm{cl}(a)|$ Divides $|G|$.

23.2 The Class Equation

Corollary 2 Class Equation

> For any finite group G,
>
> $$|G| = \sum |G : C(a)|,$$
>
> where the sum runs over one element a from each conjugacy class of G.

Theorem 23.2 p-Groups Have Nontrivial Centers

> Let G be a nontrivial finite group whose order is a power of a prime p, then $Z(G)$ has more than one element.

Proof $\mathrm{cl}(a) = \{a\}$ if and only if $a \in Z(G)$. By culling out these elements, $|G| = |Z(G)| + \sum |G : C(a)|$, since p divides both $|G|$ and $|G : C(a)| = p^k$, it also divides $Z(G)$.

Corollary Groups of Order p^2 Are Abelian

> If $|G| = p^2$, where p is prime, then G is Abelian.

Proof $|Z(G)| = p \text{ or } p^2$. If $|Z(G)| = p$, then $|G/Z(G)| = p$, so that $G/Z(G)$ is cyclic, and hence G is Abelian. (This case doesn't exist.)

23.3 The Sylow Theorems

Theorem 23.3 Existence of Subgroups of Prime-Power Order (Sylow First Theorem)

> Let G be a finite group and let p be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k.

- The converse of Lagrange's Theorem is true for all finite Abelian groups and all finite groups of prime-power order.

Definition Sylow p-Subgroup

> Let G be a finite group and let p be a prime. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, then any subgroup of G of order p^k is called a **Sylow p-subgroup** of G.

Corollary Cauchy's Theorem

> Let G be a finite group and let p be a prime that divides the order of G, then G has an element of order p.

Definition Conjugate Subgroups

> Let H and K be subgroups of a group G, we say that H and K are **conjugate** in G if there is an element g in G such that $H = gKg^{-1}$.

Recall that

- $\mathrm{orb}_G(i) = \{\phi(i) \mid \phi \in G\}$, and $|\mathrm{orb}_G(i)|$ divides $|G|$.
- $N(H) = \{x \in G \mid xHx^{-1} = H\}$.
- Conjugation is an automorphism.

Theorem 23.4 Sylow's Second Theorem

> If H is a subgroup of a finite group G and $|H|$ is a power of a prime p, then H is contained in some Sylow p-subgroup of G.

Theorem 23.5 Sylow's Third Theorem

> Let p be a prime and let G be a group of order $p^k m$, where p does not divide m. Then the number n of Sylow p-subgroups of G is equal to 1 modulo p and divides m. Furthermore, any two Sylow p-subgroups of G are conjugate.

- Let K_1 be any Sylow p-subgroup of G and let $C = \{K_1, K_2, \cdots, K_n\}$ be the set of all conjugates of K in G, then $\left|\mathrm{orb}_{T(K)}(K_i)\right| = 1$ if and only if $i = 1$.

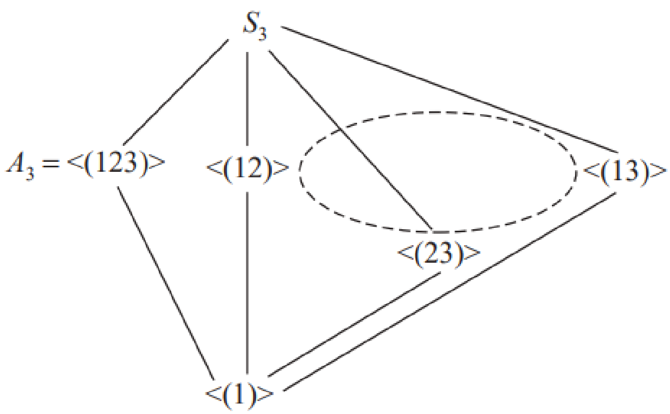
$n \equiv |C| \equiv 1 \mod p$, and $|C| = |G : N(K)|$.

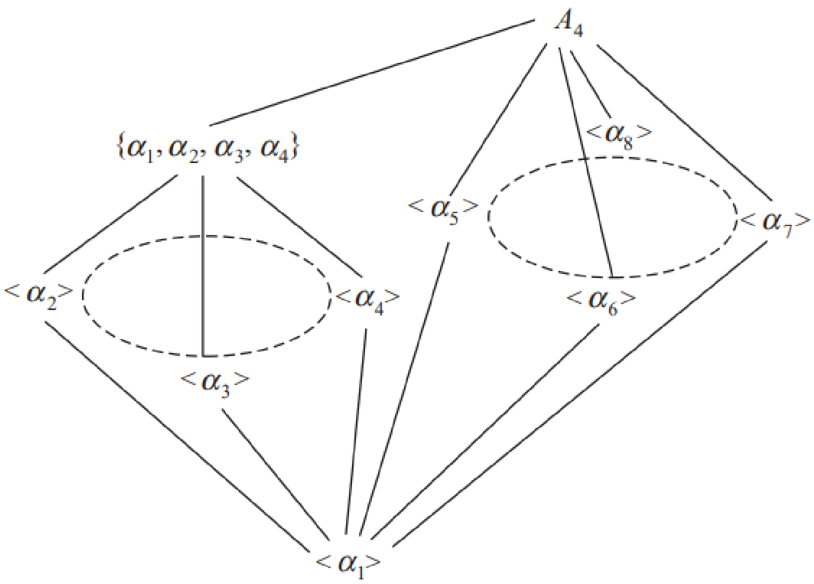
- Note that if a Sylow p-subgroup is normal, then $n_p = |G : N(K)| = |G : G| = 1$, it's also unique.

Corollary A Unique Sylow p-Subgroup Is Normal

> A Sylow p-subgroup of a finite group G is a normal subgroup of G is and only if it is the only Sylow p-subgroup of G.

- Lattices of subgroups for S_4 and A_4.





23.4 Applications of Sylow Theorems

Theorem 23.6 Cyclic Groups of Order pq

> If G is a group of order pq, where p and q are primes, $p < q$, and $p \nmid q - 1$, then G is isomorphic to $\mathbb{Z}_{pq}$.

Proof The number of Sylow p-subgroups of G is of the form $1 + kp$ and divides q, so $1 + kp = 1 \text{ or } q$, so $k = 0$, Simiarly, there is only one Sylow p-subgroup H of G, and only one Sylow q-subgroup K of G, all of which are normal, so $G = HK$ and $H \cap K = \{e\}$, thus $G = H \times K \approx \mathbb{Z}_p \oplus \mathbb{Z}_q \approx \mathbb{Z}_{pq}$.

The number of groups of any order less than 2048 is given at http://oeis.org/A000001/b000001.txt

23.5 Exercises

Sylow's Theorem ⭐

Let G be a finite group of order $p^n m$, where $p \nmid m$.

1. There exists at least one Sylow p-subgroup of G.
2. If P and Q are Sylow p-subgroups, then $\exists g \in G,\ Q = gPg^{-1}$.
3. $n_p \equiv 1 \mod p$,

   $n_p \mid m$,

   $n_p = [G : N(P)]$.

Methods ⭐

When consider a group of order n:

- Use Sylow Third Theorem.
- The number of elements of some orders can't exceed the order of the group. (May use HK to form a group.)
- Normal ($N(H) = G$)
  - If there is only one Sylow p-subgroup, then it's normal.
  - If a subgroup has index 2, then it's normal.
  - Every subgroup of a cyclic normal subgroup is normal.
  - If H and K are normal, then $N \cap M$ and HK is normal.
- If H is normal, then HK is a subgroup; if K is also normal, then $HK = H \times K$.
- $|HK| = |H|\,|K| / |H \cap K|$.
- Consider $N(H \cap H')$.
- If p divides $|G|$, then G has an element of order p.
- Groups of order p^2 are Abelian.
- $|N(H)/C(H)|$ divides $|\mathrm{Aut}\ H|$ and $N(H)$.
- If $G/Z(G)$ is cyclic, then G is Abelian.

Examples

- A group of order 72 must have a proper nontrivial normal subgroup.
- A group of order $p^2 q$ is Abelian if and only if $p \nmid q-1$ and $q \nmid p^2 - 1$.
- If $yxy^{-1} = x^i$, $|y| = 2$, then $x = y^{-1}x^i y = (yxy^{-1})^i = x^{i^2}$, so $x^{i^2-1} = e$.
- A group of order 255 is $\mathbb{Z}_{255}$.
- Exercise 40 🌙: Suppose that G is a group of order 60 and G has a normal subgroup N of order 2, then
  - G has normal subgroups of orders 6, 10, and 30.
  - G has subgroups of orders 12 and 20.
  - G has a cyclic subgroup of order 30.

  Answer is in the pdf.

Exercises

1. $\mathbb{Z}_2$ is the only group that has exactly two conjugacy classes.
2. G is not the union of all conjugates of a proper subgroup H.
3. $bab^{-1} = a^i \quad \Rightarrow \quad b^k ab^{-k} = a^{i^k}$.

4. Construct a non-Abelian group of the form $\left\{a^i b^j\right\}$ and the multiplication is defined using the relation $ba = a^i b$, then i must satisfy that $|a|$ divides $i^{|b|} - 1$ and $|b|$ divides $i^{|a|} - 1$. ⭐
5. Let H be a Sylow p-subgroup
   1. The elements of $N(H)$ whose orders are powers of p are those of H. ⭐
   2. H is the only Sylow p-subgroup of G contained in $N(H)$.
   3. $N(N(H)) = N(H)$.
6. For a p-group G of order p^n
   1. G has normal subgroups of order p^k for all k between 1 and n (inclusive). ⭐
   2. If G has exactly one subgroup for each divisor of p^n, then G is cyclic.
   3. If H is a proper subgroup of G, then $N(H) > H$.
   4. If p is the smallest prime that divides $|G|$ and H is cyclic, then $N(H) = C(H) = G$.
7. $|N(H)| = \left|N(xHx^{-1})\right|$ since $\forall n \in N(H),\ xnx^{-1} \in N(xHx^{-1})$ and vice versa. ⭐
8. Let H be a Sylow 3-subgroup of a finite group G and K be a Sylow 5-subgroup of G. If 3 divides $|N(K)|$, then 5 divides $|N(H)|$.
9. A normal p-subgroup is contained in every Sylow p-subgroup. ⭐

Question: 34, 52.

Confusino: 54, 63.

23.6 Bibliography of Ludwig Sylow

24 Finite Simple Groups

24.1 Historical Background

Definition Simple Group

> A group is **simple** if its only normal subgroups are the identity subgroup and the group itself.

- The series of simple groups $G_0/G_1, G_1/G_2, \cdots, G_{n-1}/G_n$ are called the **composition factors** of $G = G_0$.

Simple groups families examples

- The Abelian simple groups is $\mathbb{Z}_p$.
- A_n is simple for all $n \geq 5$.
- $\mathrm{PSL}(n, \mathbb{Z}_p) \equiv \mathrm{SL}(n, \mathbb{Z}_p)/Z(\mathrm{SL}(n, \mathbb{Z}_p))$ except when $n = 2$ and $p = 2 \text{ or } 3$.
- **Feit-Thompson Theorem**: A non-Abelian simple group has even order.
- The largest sporadic simple group: Monster.

24.2 Nonsimplicity Tests

Theorem 24.1 Sylow Test for Nonsimplicity

> Let n be a positive integer that is not prime, and let p be a prime divisor of n. If 1 is the only divisor of n that is equal to 1 modulo p, then there does not exist a simple group of order n.

Proof

If n is a prime-power, then a group of order n has a nontrivial center and therefore is not simple.

Else, the number of Sylow p-subgroups of a group of order n is equal to 1 modulo p and divides n. Therefore the number is 1 and hence the Sylow p-subgroup is normal.

Theorem 24.2 $2 \cdot \mathrm{Odd}$ Test

> An integer of the form $2 \cdot n$, where n is an odd number greater than 1, is not the order of a simple group.

Proof

$\phi : G \to S,\ g \mapsto T_g$, where $T_g(x) = gx$ is an isomorphism from G to its permutation group. Since $|G| = 2n$, there is an element g in G of order 2. Then, when T_g is written in disjoint cycle form, each cycle must have length 1 or 2. But 1-cycle (x) would mean $x = T_g(x) = gx$ and $g = e$. Thus T_g consists of exactly n transpositions. Therefore T_g is an odd permutation. This means that the set of even permutation has index 2 and hence normal.

Theorem 24.3 Generalized Cayley Theorem

> Let G be a group and let H be a subgroup of G. Let S be the group of all permutations of the left cosets of H in G. Then there is a homomorphism from G into S whose kernel lies in H and contains every normal subgroup of G that is contained in H.

Proof

Define $T_g(xH) = gxH$, then $\alpha : g \mapsto T_g$ is a homomorphism from G into S.

If $g \in \operatorname{Ker}\alpha$, then $H = T_g(X) = gH$, thus $g \subseteq H$.

If K is normal and $K \subseteq H$, then $kx = xk'$, $T_k(xH) = kxH = xk'H = xH$ is a identity permutation, thus $k \in \operatorname{Ker}\alpha$.

- The kernel itself is a normal subgroup.
- If $|G : H| = p$, where p is the smallest prime divisor of G, then H is normal.

Corollary 1 Index Theorem

> If G is a finite group and H is a proper subgroup of G such that $|G|$ does not divide $|G : H|!$, then H contains a nontrivial normal subgroup of G. In particular, G is not simple.

Proof

$\operatorname{Ker}\alpha$ is a normal subgroup of G contained in H and $G/\operatorname{Ker}\alpha$ is isomorphic to a subgroup of S. Thus, $|G/\operatorname{Ker}\alpha| = |G|/|\operatorname{Ker}\alpha|$ divides $|S| = |G : H|!$, and the order of $\operatorname{Ker}\alpha$ must be greater than 1.

Corollary 2 Embedding Theorem

> If a finite non-Abelian simple group G has a subgroup of index n, then G is isomorphic to a subgroup of A_n.

Non-Abelian simple groups of order less than 200:

- Icosahedral (Or dodecahedron) group: A_5.

- $\mathrm{PSL}(2, \mathbb{Z}_7) = \mathrm{SL}(2, \mathbb{Z}_7)/Z(\mathrm{SL}(2, \mathbb{Z}_7))$.

- Every group is isomorphic to a subgroup of S_n for some n (Cayley's Theorem), and S_n is a subgroup of A_{n+2}, so every group is isomorphic to a subgroup of a finite simple group.

24.3 The Simplicity of A_5

24.4 The Fields Medal

24.5 The Cole Prize

24.6 Exercises

Methods

- Theorems
  - Sylow's Theorems. ($n_p = |G : N(H_p)|$)
  - $2 \cdot \mathrm{Odd}$ Test.
  - Index Theorem. (Consider $|N(H)|$.)
  - Embedding Theorem. (Find impossible orders.)
  - $|N(H)/C(H)| = |\mathrm{Inn}\, H|$ divides $|\mathrm{Aut}\, H|$.
- If $|H| = p^2$, $|N(H \cap H')| \geq |HH'| = |H|\,|H'|/\,|H \cap H'|$.
- Every group of order 30 has an element of order 15.
- If $\gcd(|x|, |G/H|) = 1$, then $x \in H$.
- Consider the subgroup L of another prime q of $N(L_p)$, then $N(L) \geq N(L_p)$ and $N(L) \geq N(L_q)$.
- Every proper subgroup H of a p-group G is a proper subgroup of $N(H)$, i.e. $N(H) > H$.

Exercise

1. There is no simple group of order pqr, where p, q and r are primes (need not to be distinct).
2. If H is a proper normal subgroup of largest order of G, then G/H is simple.
3. If H and K are subgroups of a finite simple group G such that $|G : H|$ and $|G : K|$ are prime, then $|H| = |K|$.
4. If there is a non-trivial homomorphism from a finite group G to S_n where $|G| > n!$, then G is not simple.
5. A group of order $p^n m$, where $m < 9$ or m is a prime, has a normal subgroup of order p^{n-1} or p^n.

Quesetion: 8, 26

24.7 Bibliography of Michael Aschbacher

24.8 Bibliography of Daniel Gorenstein

24.9 Bibliography of John Thompson

25 Generators and Relations

25.1 Motivation

25.2 Definitions and Notation

- For any set $S = \{a, b, c, \cdots\}$, define $S^{-1} = \{a^{-1}, b^{-1}, c^{-1}, \cdots\}$, $W(S) = \{x_1 x_2 \cdots x_k \mid x_i \in S \cup S^{-1}, k \in \mathbb{N}\}$.
- The elements in $W(S)$ is called **words** from S, and the word is called the **empty word** e when $k = 0$.
- Define a binary operation such that $\forall x, y \in W(S), xy \in W(S)$.
- Notice that aa^{-1} is not e, $(ab)^{-1}$ is not $b^{-1}a^{-1}$.

Definition Equivalence Classes of Words

> For any pair of elements u and v of $W(S)$, we say that u is **related** to v if v can be obtained from u by a finite sequence of insertions or deletions of words of the form xx^{-1} of $x^{-1}x$, where $x \in S$.

25.3 Free Group

Theorem 25.1 Equivalence Classes Form a Group

> Let S be a set of distinct symbols. For any word u in $W(S)$, let $\bar{u}$ denote the set of all words in $W(S)$ equivalent to u. Then the set of all equivalence classes of elements of $W(S)$ is a group under the operation $\overline{u} \cdot \overline{v} = \overline{uv}$.

Theorem 25.2 Universal Mapping Property

> Every group is a homomorphic image of a free group.

Corollary Universal Factor Group Property

> Every group is isomorphic to a factor group of a free group.

25.4 Generators and Relations

Definition Generators and Relations

> Let G be a group generated by some subset $A = \{a_1, a_2, \cdots, a_n\}$ and let F be the free group on A. Let $W = \{w_1, w_2, \cdots, w_t\}$ be a subset of F and let N be the smallest normal subgroup of F containing W. We say that G is given by the generators $a_1, a_2, \cdots, a_n$ and the relations $w_1 = w_2 = \cdots = w_t = e$ if there is an isomorphism from F/N onto G that carries $a_i N$ to a_i.

- $G = \langle a_1, a_2, \cdots, a_n \mid w_1 = w_2 = \cdots = w_t = e \rangle$, and the RHS is called the **presentation**.
- The only nontrivial Abelian group that is free: $\mathbb{Z} \approx \langle a \rangle$.

Theorem 25.3 Dyck's Theorem (1882)

> Let $G_1 = \langle a_1, a_2, \cdots, a_n \mid w_1 = w_2 = \cdots = w_t = e \rangle$, and $G_2 = \langle a_1, a_2, \cdots, a_n \mid w_1 = w_2 = \cdots = w_t = w_{t+1} = \cdots = w_{t+k} = e \rangle$, then G_2 is a homomorphic image of G_1.

Corollary Largest Group Satisfying Defining Relations

> If K is a group satisfying the defining relations of a finite group G and $|K| \geq |G|$, then $K \approx G$.

25.5 Classification of Groups of Order Up to 15

Theorem 25.4 Classification of Groups of Order 8 (Cayley, 1859)

> Up to isomorphism, there are only five groups of order 8:
> $\mathbb{Z}_8, \mathbb{Z}_4 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, D_4, Q_4$ (quaternions).

- Quaternions: $Q_4 = \langle a, b \mid a^2 = b^2 = (ab)^2 \rangle$.
- **Dicyclic group** of order $4n$: $Q_{2n} = \langle a, b \mid a^{2n} = e, a^n = b^2, b^{-1}ab = a^{-1} \rangle$, $Z(Q_{2n}) = \{e, x^n\}$, $Q_{2n}/Z(Q_{2n}) \approx D_n$.

25.6 Characterization of Dihedral Groups

Theorem 25.5 Characterization of Dihedral Groups

> Any group generated by a pair of elements of order 2 is dihedral.

- $D_n \approx \langle x, y \mid x^2 = y^n = e, xyx = y^{-1} \rangle$.
- In D_∞, $|xy^i| = 2$, $|y^i| = \infty$, $0 \neq i \in \mathbb{Z}$.

25.7 Exercises

1. $D_4 \approx \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{Z}_2 \right\}$.

25.8 Bibliography of Marshall Hall, Jr.

26 Symmetry Groups

26.1 Isometries

Definition Isometry

> An **isometry** of n-dimensional space $\mathbb{R}^n$ is a function from $\mathbb{R}^n$ onto $\mathbb{R}^n$ that preserves distance.

Definition Symmetry Group of a Figure in $\mathbb{R}^n$

> Let F be a set of points in $\mathbb{R}^n$, then the **symmetry group** of F in $\mathbb{R}^n$ is the set of all isometries of $\mathbb{R}^n$ that carry F onto itself, whose operation is function composition.

Every isometry of $\mathbb{R}^2$ is one of four types:

- Rotation, reflection (mirror), translation, glide-reflection.

26.2 Classification of Finite Plane Symmetry Groups

Theorem 26.1 Finite Symmtry Groups in the Plane

> The only finite plane symmetry gruops are $\mathbb{Z}_n$ and D_n.

26.3 Classification of Finite Groups of Roation in $\mathbb{R}^3$

Theorem 26.2 Finite Gruops of Rotations in $\mathbb{R}^3$

> Up to isomorphism, the finite groups of rotations in $\mathbb{R}^3$ are $\mathbb{Z}_n, D_n, A_4, S_4$ and A_5.

26.4 Exercises

Confusion: 9

27 Symmetry and Counting

27.1 Motivation

27.2 Burnside's Theorem

Definition Elements Fixed by ϕ

> For any group G of permutations on a set S and any ϕ in G, we let
> $\text{fix}(\phi) = \{i \in S \mid \phi(i) = i\}$.

Theorem 27.1 Burnside's Theorem

> If G is a finite group of pertations on a set S, then the number of orbits of elements of S under G is
>
> $$n = \frac{1}{|G|} \sum_{\phi \in G} |\text{fix}(\phi)|.$$

Proof Let N denote the number of pairs (ϕ, i), $\phi \in G, u \in S$, $\phi(i) = i$, and count these pairs in two ways:

$$\begin{aligned} N = \sum_{\phi \in G} |\text{fix}(\phi)| &= \sum_{i \in S} |\text{stab}_G(i)| \\ &= \sum_{\text{orb}_G(s), s \in S} \left(\sum_{t \in \text{orb}_G(s)} |\text{stab}_G(t)| \right) \\ &= \sum_{\text{orb}_G(s), s \in S} |\text{orb}_G(s)| \, |\text{stab}_G(s)| \\ &= \sum_{\text{orb}_G(s), s \in S} |G| = n \cdot |G|. \end{aligned}$$

27.3 Applications

27.4 Group Action

e.g. $\gamma : \text{GL}(n, \mathbb{F}) \to S := \{(a_i)_{n \times 1} \mid a_i \in \mathbb{F}\}$, $g \mapsto \gamma_g$.

27.5 Exercises

27.6 Bibliogrphy of William Burnside

28 Cayley Digraphs of Groups

28.1 Motivation

28.2 The Cayley Digraph of a Group

Definition Cayley Digraph of a Group

> Let G be a finite group and let S be a set of generators for G. We define a digraph (directed graph) $\mathrm{Cay}(S:G)$, called the **Cayley digraph** of G with generating set S, as follows:
>
> 1. Each element of G is a **vertex** of $\mathrm{Cay}(S:G)$.
> 2. $\forall x, y \in G$, there is an **arc** from x to y if and only if $\exists s \in S,\ \mathrm{s.t.}\ xs = y$.

28.3 Hamiltonian Circuits and Paths

Theorem 28.1 A Necessary Condition

> $\mathrm{Cay}(\{(1,0),(0,1)\} : \mathbb{Z}_m \oplus \mathbb{Z}_n)$ does not have a Hamiltonian circuit when $\gcd(m,n) = 1,\ m,n > 1$.

Theorem 28.2 A Sufficient Condition

> $\mathrm{Cay}(\{(1,0),(0,1)\} : \mathbb{Z}_m \oplus \mathbb{Z}_n)$ has a Hamiltonian circuit when $n \mid m$.

- This Hamiltonian circuit can be denoted by $m * [(n-1) * (0,1), (0,1)]$.

Theorem 28.3 Abelian Groups Have Hamiltonian Paths

> Let G be a finite Abelian group, and let S be any generating set for G, then $\mathrm{Cay}(S:G)$ has a Hamiltonian path.

- $(a_1, a_2, \cdots, a_k, s, a_1, a_2, \cdots, a_k, s, \cdots, a_1, a_2, \cdots, a_k, s, a_1, a_2, \cdots, a_k)$.
- It can be generalized to include all **Hamiltonian groups**, all of whose subgroups are normal. (One non-Abelian example is Q_4.)
- $\forall m, n \in \mathbb{N}^+,\ \mathrm{Cay}(\{(r,0),(f,0),(e,1)\} : D_n \oplus \mathbb{Z}_m)$ has a Hamiltonian circuit.

28.4 Some Applications

28.5 Exercises

Confusion: 36.

28.6 Bibliography of William Rowan Hamilton

28.7 Bibliography of Paul Erdos

29 Introduciton to Algebraic Coding Theory

29.1 Motivation

- **Hamming (7, 4) Code**

  Multiply each of the 4-tuples on the right by the matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

29.2 Linear Codes

Definition Linear Code

> An (n, k) **linear code** over a finite field $\mathbb{F}$ is a k-dimensional subspace V of the vector space $\mathbb{F}^n = \underbrace{\mathbb{F} \oplus \mathbb{F} \oplus \cdots \oplus \mathbb{F}}_{n \text{ copies}}$ over $\mathbb{F}$. The members of V are called the **code words**. When $\mathbb{F} = \mathbb{Z}_2$, the code is called **binary**. When $\mathbb{F} = \mathbb{Z}_3$, the code is called **ternary**.

- In a binary linear code
  - For all digits, either all the code words are 0, or exactly half of them are 0.
  - Either every member has even weight, or exactly half of them has even weight.

Definition Hamming Distance, Hamming Weight

> The **Hamming distance** between two vectors in $\mathbb{F}^n$ is the number of components in which they differ. The **Hamming weight** of a vector is the number of nonzero components of the vector. The **Hamming weight** of a linear code is the minimum weight of any nonzero vector in the code.

- Hamming distance: $d(u, v)$.
- Hamming weight: $\mathrm{wt}(u)$.

Theorem 29.1 Properties of Hamming Distance and Hamming Weight

> 1. $d(u, v) \le d(u, w) + d(w, v)$.
> 2. $d(u, v) = \mathrm{wt}(u - v)$.

- $d(u, v) = d(v, u)$.
- $d(u, v) = 0 \quad \Leftrightarrow \quad u = v$.
- $d(u, v) = d(u + w, v + w)$.

Theorem 29.2 Correcting Capability of a Linear Code

> If the Hamming weight of a linear code is at least $2t + 1$ $(t \in \mathbb{Q}^+)$, then the code can correct any t or fewer errors. Alternatively, the same code can detect any $2t$ or fewer errors.

Proof 1. For a transmitted code word u and a received code word v, consider a code word other than u, then

$$2t + 1 \le \mathrm{wt}(w - u) = d(w, u) \le d(w, v) + d(v, u) \le d(w, v) + t,$$

so the code word closest to v is u.

2. $d(u, v) \le 2t$, but the minimum distance between distinct code words is at least $2t + 1$.

- The converse of Theorem 29.2 is also true.
- We can't do both simultaneously.

- If we write the Hamming weight of a linear code in the form $2t+s+1$, we can correct any t or fewer errors and detect any $t+s$ or fewer erros. ⭐
- For example, for a code with Hamming weight 5, we have options as follows
  1. Detect any four errors ($t=0, s=4$).
  2. Correct any one error and detect any two or three errors ($t=1, s=2$).
  3. Correct any two errors ($t=2, s=0$).
- A matrix of the following form is called the **standard generator matrix** (or **standard encoding matrix**), which produces a **systematic code**.

$$G=\left(\begin{array}{cccc|ccc} 1 & 0 & \cdots & 0 & a_{11} & \cdots & a_{1,n-k} \\ 0 & 1 & \cdots & 0 & a_{21} & \cdots & a_{2,n-k} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & a_{k1} & \cdots & a_{k,n-k} \end{array}\right).$$

29.3 Parity-Check Matrix Decoding

If there is only one error:

Suppose that V is a systematic linear code over the field $\mathbb{F}$ given by the standard generator matrix $G=[I_k|A]$, then $H=\left[\dfrac{-A}{I_{n-k}}\right]$ is the **parity-check matrix** for V.

1. For any received word w, compute wH.
2. If wH is the zero vector, assume that no error was made.
3. If there is exactly one instance of a nonzero element $s\in\mathbb{F}$ and a row i of H such that $wH=sH_i$, assume that the sent word was $w-(0\cdots s\cdots 0)$, where s occurs in the i^{th} component.

   (When the code is binary, if wH is the i^{th} row of H for exactly one i...)

- It cannot detect any multiple errors, and we have restrictions on the parity-check matrix.

Lemma 29.1 Orthogonality Relation

> Let C be a systematic (n,k) linear code over $\mathbb{F}$ with a standard generator matrix G and parity-check matrix H. Then, for any vector v in $\mathbb{F}^n$, we have $vH=\mathbf{0}\Leftrightarrow v\in C$.

Proof $\dim(\text{Ker } H)=k$,

$$GH=[I_k|A]\left[\frac{-A}{I_{n-k}}\right]=-A+A=[0]\quad\text{(the zero matrix)}$$
$$vH=(mG)H=m[0]=0\quad\text{(the zero vector)}$$

Theorem 29.3 Parity-Check Matrix

> Parity-check matrix decoding will correct any single error if and only if the rows of the parity-check matrix are nonzero and no one row is a scalar multiple of any other row.

Proof $(w+e_i)H=wH+e_iH=e_iH$.

29.4 Coset Decoding

- Construct a table called a **standard array** whose words in the first column are called the **coset leaders**.

- A table of an (n,k) linear code over a field with q elemnts will have $|C| = q^k$ columns and $|V:C| = q^{n-k}$ rows.

Theorem 29.4 Coset Decoding Is Nearest-Neighbor Decoding

> In coset decoding, a received word w is decoded as a code word c such that $d(w,c)$ is a minimum.

Proof Suppose that v is the coset leader for the coset $w+C$, then $w+C = v+C$, $w = v+c$ for some $c \in C$. Now, if c' is any code word, then $w - c' \in w + C = v + C$, $\mathrm{wt}(w-c') \geq \mathrm{wt}(v+C) = \mathrm{wt}(v)$, therefore

$$d(w,c') = \mathrm{wt}(w-c') \geq \mathrm{wt}(v) = \mathrm{wt}(w-c) = d(w,c).$$

Definition Syndrome

> If an (n,k) linear code over $\mathbb{F}$ has parity-check matrix H, then, for any vector u in $\mathbb{F}^n$, the vector uH is called the **syndrome** of u.

Theorem 29.5 Same Coset—Same Syndrome

> Let C be an (n,k) linear code over $\mathbb{F}$ with a parity-check matrix H. Then, two vectors of $\mathbb{F}^n$ are in the same coset of C if and only if they have the same syndrome.

Proof $u, v \in w + C \quad \Leftrightarrow \quad u - v \in C \quad \Leftrightarrow \quad 0 = (u-v)H = uH - vH.$

Steps

1. Calculate the syndrome wH.
2. Find the coset leader v such that $wH = vH$.
3. Assume that the vector sent was $w - v$.

29.5 Historical Note

29.6 Exercises

Methods

1. Nearest-neighbor method.
2. Parity-check matrix method.
3. Coset decoding using a standard array.
4. Coset decoding using the syndrome method.

29.7 Bibliography of Richard W.Hamming

29.8 Bibliography of Jessie mac Williams

29.9 Bibliography of Vera Pless

30 An introduction to Galois Theory

30.1 Fundamental Theorem of Galois Theory

Definitions Automorphism, Galois Group, Fixed Field of H

> Let $\mathbb{E}$ be an extension field of the field $\mathbb{F}$. An **automorphism** of $\mathbb{E}$ is a ring isomorphism from $\mathbb{E}$ onto $\mathbb{E}$. The **Galois group** of $\mathbb{E}$ over $\mathbb{F}$, $\text{Gal}(\mathbb{E}/\mathbb{F})$, is the set of all automorphisms of $\mathbb{E}$ that take every element of $\mathbb{F}$ to itself. If H is a subgroup of $\text{Gal}(\mathbb{E}/\mathbb{F})$, then the set
>
> $$\mathbb{E}_H = \{x \in \mathbb{E} \mid \phi(x) = x \text{ for all } \phi \in H\}$$
>
> is called the **fixed field** of H.

- Let $\mathscr{F}$ be the lattice of subfields of $\mathbb{E}$ containing $\mathbb{F}$, and let $\mathscr{G}$ be the lattice of subgroups of $\text{Gal}(\mathbb{E}/\mathbb{F})$, then

$$g: \begin{array}{c} \mathscr{F} \to \mathscr{G} \\ \mathbb{K} \mapsto \text{Gal}(\mathbb{E}/\mathbb{K}) \end{array} \qquad f: \begin{array}{c} \mathscr{G} \to \mathscr{F} \\ H \mapsto \mathbb{E}_H \end{array}$$

- $\mathbb{K} \subseteq \mathbb{L} \quad \Rightarrow \quad g(\mathbb{K}) \supseteq g(\mathbb{L})$.
- $G \subseteq H \quad \Rightarrow \quad f(G) \supseteq f(H)$.
- $\forall \mathbb{K} \in \mathscr{F},\ (fg)\mathbb{K} \supseteq \mathbb{K}$.
- $\forall G \in \mathscr{G},\ (fg)G \supseteq G$.

Theorem 30.1 Fundamental Theorem of Galois Theory

> Let $\mathbb{F}$ be a field of characteristic 0 or a finite field. If $\mathbb{E}$ is the splitting field over $\mathbb{F}$ for some polynomial in $\mathbb{F}[x]$, then $g: \mathscr{F} \to \mathscr{G},\ \mathbb{K} \mapsto \text{Gal}(\mathbb{E}/\mathbb{K})$ is a one-to-one correspondence. Furthermore, for any subfield $\mathbb{K}$ of $\mathbb{E}$ containing $\mathbb{F}$,
>
> 1. $[\mathbb{E} : \mathbb{K}] = |\text{Gal}(\mathbb{E}/\mathbb{K})|,\ [\mathbb{K} : \mathbb{F}] = |\text{Gal}(\mathbb{E}/\mathbb{F})| / |\text{Gal}((\mathbb{E}/\mathbb{K}))|$.
>
>   (The index of $\text{Gal}(\mathbb{E}/\mathbb{K})$ in $\text{Gal}(\mathbb{E}/\mathbb{F})$ equals the degree of $\mathbb{K}$ over $\mathbb{F}$.)
> 2. If $\mathbb{K}$ is the splitting field of some polynomimal in $\mathbb{F}[x]$, then $\text{Gal}(\mathbb{E}/\mathbb{K})$ is a normal subgroup of $\text{Gal}(\mathbb{E}/\mathbb{F})$, and $\text{Gal}(\mathbb{K}/\mathbb{F}) \approx \text{Gal}(\mathbb{E}/\mathbb{F}) / \text{Gal}(\mathbb{E}/\mathbb{K})$.
> 3. $\mathbb{K} = \mathbb{E}_{\text{Gal}(\mathbb{E}/\mathbb{K})}$. (The fixed field of $\text{Gal}(\mathbb{E}/\mathbb{K})$ is $\mathbb{K}$.)
> 4. If H is a subgroup of $\text{Gal}(\mathbb{E}/\mathbb{F})$, then $H = \text{Gal}(\mathbb{E}/\mathbb{E}_H)$.
>
>   (The automorphism group of $\mathbb{E}$ fixing $\mathbb{E}_H$ is H.)

- $\text{Gal}(\text{GF}(p^n)/\text{GF}(p)) \approx \mathbb{Z}_n$.

  Proof Say $\mathbb{F} = \text{GF}(p)$, $\text{GF}(p^n) = \mathbb{F}(b)$, where b is the zero of an irreducible polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ a_i \in \mathbb{F}$.

  $p(b) = 0 = \phi(p(b)) = p(\phi(b))$, so there are at most n possibilities for $\phi(b)$.

  $\sigma : \mathbb{E} \to \mathbb{E},\ a \mapsto a^p$ is an automorphism, and $\mathbb{E}^*$ is cyclic, so $|\sigma|$ has order n.

  Thus, $\text{Gal}(\text{GF}(p^n)/\text{GF}(p)) \approx \mathbb{Z}_n$.

30.2 Solvability of Polynomials by Radicals

Definition Solvable by Radicals

> Let $\mathbb{F}$ be a field, and let $f(x) \in \mathbb{F}[x]$. We say that $f(x)$ is **solvable by radicals** over $\mathbb{F}$ if $f(x)$ splits in some extension $\mathbb{F}(a_1, a_2, \cdots, a_n)$ of $\mathbb{F}$ and there exist positive integers $k_1, k_2, \cdots, k_n$ such that $a_1^{k_1} \in \mathbb{F}$ and $a_i^{k_i} \in \mathbb{F}(a_1, a_2, \cdots, a_{n-1})$ for $i = 2, 3, \cdots, n$.

Definition Solvable Group

> We say that a group G is solvable if G has a series subgroups

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_k = G,$$

where for each $0 \le i < k$, H_i is normal in H_{i+1} and H_{i+1}/H_i is Abelian.

- If G is a finite solvable group, then there exist subgroups of G

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_n = G$$

  such that H_{i+1}/H_i has prime order.
- A subgroup of a solvable group is solvable.

Examples

- Solvable groups: Abelian groups, dihedral groups, groups of orde p^n.
- Every group of odd order is solvable. (Feit-Thompson Theorem)
- Any non-Abelian simple group is not solvable.
- S_n is solvable if and only if $n \le 4$.

Theorem 30.2 Condition for $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ to be Solvable

> Let $\mathbb{F}$ be a field of characteristic 0 and let $a \in \mathbb{F}$. If $\mathbb{E}$ is the splitting field of $x^n - a$ over $\mathbb{F}$, then the Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is solvable.

Theorem 30.3 Factor Group of a Solvable Group Is Solvable

> A factor group of a solvable group is solvable.

Theorem 30.4 N and G/N Solvable Implies G is Solvable

> Let N be a normal subgroup of a group G. If both N and G/N are solvable, then G is solvable.

Theorem 30.5 Solvable by Radicals Implies Solvable Group (Galois)

> Let $\mathbb{F}$ be a field of characteristic 0 and let $f(x) \in \mathbb{F}[x]$. Suppose that $f(x)$ splits in $\mathbb{F}(a_1, a_2, \cdots, a_t)$, where $a_1^{n_1} \in \mathbb{F}$ and $a_i^{n_i} \in \mathbb{F}(a_1, a_2, \cdots, a_{i-1})$ for $i = 2, 3, \cdots, t$. Let $\mathbb{E}$ be the splitting field for $f(x)$ over $\mathbb{F}$ in $\mathbb{F}(a_1, a_2, \cdots, a_t)$, then the Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is solvable.

- The converse is true also: if $\mathbb{E}$ is the splitting field of a polynomial $f(x)$ over a field $\mathbb{F}$ of characteristic 0 and $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is solvable, then $f(x)$ is solvable by radicals over $\mathbb{F}$.
- Every finite group is a Galois group over some field.
- Every solvable group is a Galois group over $\mathbb{Q}$.

30.3 Insolvability of a Quintic

30.4 Exercises

1. Let $f(x) \in \mathbb{F}[x]$ and let the zeros of $f(x)$ be $a_1, a_2, \cdots, a_n$. If $\mathbb{K} = \mathbb{F}(a_1, a_2, \cdots, a_n)$, then $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is isomorphic to a group of the a_i's, i.e., a subgroup of S_n.

31 Cyclotomic Extensions

31.1 Motivation

31.2 Cyclotomic Polynomials

- n^{th} **cyclotomic extension** of $\mathbb{Q}$: $\mathbb{Q}(\mathrm{e}^{2\mathrm{i}\pi/n})$.
- The irreducible factors of $x^n - 1$ over $\mathbb{Q}$ are called the **cyclotomic polynomials**.
- ω^k where $\gcd(n, k) = 1$ are called the **primitive n^{th} roots of unity**.

Definition Cyclotomic Polynomial

> For any positive integer n, let $\omega_1, \omega_2, \cdots, \omega_{\phi(n)}$ denote the primitive n^{th} roots of unity. The n^{th} **cyclotomic polynomial** over $\mathbb{Q}$ is the polynomial
>
> $$\Phi_n(x) = (x - \omega_1)(x - \omega_2) \cdots (x - \omega_{\phi(n)}).$$

- $\deg(\Phi_n(x)) = \phi(n)$.
- $\Phi_n(0) = 1 \ (n > 1)$.

Theorem 31.1 $x^n - 1 = \prod_{d|n} \Phi_d(x)$

> For every positive integer n, $x^n - 1 = \prod_{d|n} \Phi_d(x)$, where the product runs over all positive divisors d of n.

- It can be used to find the irreducible factorization of $x^n - 1$ over $\mathbb{Z}_p$.

Theorem 31.2 $\Phi_d(x)$ Has Integer Coefficients

> For every positive integer n, $\Phi_n(x)$ has integer coefficients.

Theorem 31.3. $\Phi_d(x)$ Is Irreducible Over $\mathbb{Z}$ (Gauss)

> The cyclotomic polynomial $\Phi_n(x)$ are irreducible over $\mathbb{Z}$.

Theorem 31.4 $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \approx U(n)$

> Let ω be a primitive n^{th} root of unity, then $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \approx U(n)$.

31.3 The Constructible Reugular *n*-gons

Lemma $\mathbb{Q}(\cos(2\pi/n)) \subseteq \mathbb{Q}(\omega)$

> Let $\omega = \mathrm{e}^{2\mathrm{i}\pi/n}$, $n \in \mathbb{N}^+$, then $\mathbb{Q}(\cos 2\pi/n) \subseteq \mathbb{Q}(\omega)$.

Theorem 31.5 Construciblity Criteria for a Regular n

> It is possible to construct the regular n-gon with a straightedge and compass if and only if n has the form $2^k p_1 p_2 \cdots p_t$, $k \geq 0$ and the p_i's are distinct primes of the form $2^m + 1$ (or $2^{2^m} + 1$).

31.4 Exercises

1. $\prod_{k=1}^{n} \mathrm{e}^{2k\mathrm{i}\pi/n} = (-1)^{n+1}$.
2. If $p = 2^n + 1 \ (n \in \mathbb{N}^+)$ is a prime, then $p = 2^{2^k} + 1$ for some $k \in \mathbb{N}$.
3. If a field contains n^{th} roots of unity for n odd, then it also contains $2n^{\text{th}}$ roots of unity. Furthermore, $\Phi_{2n}(x) = \Phi_n(-x) \ (n > 1)$. ⭐
4. $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$. ⭐

5. $p \nmid n \Rightarrow \Phi_{pn} = \Phi_n(x^p)/\Phi_n(x)$. ⭐

31.5 Bibliography of Carl Friedrich Gauss

31.6 Bibliography of Manjul Bhargava