Title

D. Zack Garza

August 17, 2019

Contents

1 List of Topics

Chapters 1-9 of Dummit and Foote

- Left and right cosets
- Lagrange's theorem
- Isomorphism theorems
- Group generated by a subset
- Structure of cyclic groups
- Composite groups
  - HK is a subgroup iff $HK = KH$
- Normalizer
  - $HK \leq H$ if $H \leq N_G(K)$
- Symmetric groups
  - Conjugacy classes are determined by cycle types
- Group actions
  - Actions of G on X are equivalent to homomorphisms from G into Sym(X)
- Cayley's theorem
- Orbits of an action
- Orbit stabilizer theorem
- Orbits act on left cosets of subgroups
- Subgroups of index p, the smallest prime dividing $|G|$, are normal
- Action of G on itself by conjugation
- Class equation
- p-groups
  - Have non trivial center
- p^2 groups are abelian
- Automorphisms, the automorphism group
  - Inner automorphisms
  - $Inn(G) \cong Z/Z(G)$
  - $Aut(S_n) = Inn(S_n)$ unless $n = 6$
  - $Aut(G)$ for cyclic groups
  - $G \cong Z_p^n$, then $Aut(G) \cong GL_n(Z_p)$
- Proof of Sylow theorems
- A_n is simple for $n \geq 5$

- Recognition of internal direct product
- Recognition of semi-direct product
- Classifications:
  - pq
- Free group & presentations
- Commutator subgroup
- Solvable groups
  - S_n is solvable for $n \leq 4$
- Derived series
  - Solvable iff derived series reaches e
- Nilpotent groups
  - Nilpotent iff all sylow-p subgroups are normal
  - Nilpotent iff all maximal subgroups are normal
- Upper central series
  - Nilpotent iff series reaches G
- Lower central series
  - Nilpotent iff series reaches e
- Fratini's argument
- Rings
  - I maximal iff R/I is a field
  - Zorn's lemma
  - Chinese remainer theorem
  - Localization of a domain
  - Field of fractions
  - Factorization in domains
  - Euclidean algorithm
  - Gaussian integers
  - Primes and irreducibles
  - Domains
    * Primes are irreducible
  - UFDs
    * Have GCDs
    * Sometimes PIDs
  - PIDs
    * Noetherian
    * Irreducibles are prime
    * Are UFDs
    * Have GCDs
  - Euclidean domains
    * Are PIDs
  - Factorization in $Z[i]$
  - Polynomial rings
  - Gauss' lemma
  - Remainder and factor theorem
  - Polynomials
  - Reducibility
  - Rational root test
  - Eisenstein's criterion

2 Groups

2.1 Definitions

2.1.1 Subgroup Generated by a set A

- $\langle A \rangle = \{a_1^{\pm 1}, a_2^{\pm 1}, \cdots a_2^{\pm 1} : a_i \in A, n \in \mathbb{N}\}$
- Equivalently, the intersection of all H such that $A \subseteq H \leq G$

2.1.2 Free Group on a set X

- Equivalently, words over the alphabet X made into a group via concatenation

2.1.3 Centralizer of an element or a subgroup

- $C_G(a) = \{g \in G : ga = ag\}$
-
$$C_G(H) = \{g \in G : \forall h \in H, gh = hg\} = \bigcap_{h \in H} C_G(h)$$
  - Note - requires the same g on both sides!
- Facts:
  - $C_G(H) \leq G$
  - $C_G(H) \trianglelefteq N_G(H)$
  - $C_G(G) = Z(G)$
  - $C_H(a) = H \bigcap C_G(a)$

2.1.4 Center of a group

- $Z(G) = \{g \in G : \forall x \in G, gx = xg\}$
- Facts
  -
$$Z(G) = \bigcap_{a \in G} C_G(a)$$

2.1.5 Normalizer of a subgroup

-
$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$
- Equivalently, $\bigcup\{K : H \trianglelefteq K \leq G\}$ (the largest $K \leq G$ for which $H \trianglelefteq K$)
- Equivalently, the stabilizer of H under G acting on its subgroups via conjugation
- Differs from centralizer; can have $gh = h'g$
- Facts:
  - $C_G(H) \subseteq N_G(H) \leq G$
  - $N_G(H)/C_G(H) \cong A \leq Aut(H)$

- Given $H \subseteq G$, let

$$S(H) = \bigcup_{g \in G} gHg^{-1}$$

, so $|S(H)|$ is the number of conjugates to H. Then

$$|S(H)| = [G : N_G(H)]$$

  * i.e. the number of subgroups conjugate to H equals the index of the normalizer of H.

2.1.6 Normal Core of a subgroup

- $$H_G = \bigcap_{g \in G} gHg^{-1}$$
- Equivalently, $H_G = \langle N : N \trianglelefteq G \ \& \ N \leq H \rangle$
  - Largest normal subgroup that contains H
- Equivalently, $H_G = \ker\psi$ where $\psi : G \to Sym(G/H);\ g \sim (xH) = (gx)H$
- Facts:
  - $H_G \trianglelefteq G$ and is an idempotent operation

2.1.7 Normal Closure of a subgroup

- $H^G = \{gHg^{-1} : g \in G\}$
- Equivalently,

$$H^G = \bigcap \{N : H \leq N \trianglelefteq G\}$$

  - (The smallest normal subgroup of G containing H)

2.1.8 Group Action of a group on a set

- Given as a function

$$\phi : G \times X \to X(g, x) \mapsto g \sim x$$

which gives rise to a function

$$\phi_g : X \to Xx \mapsto g \sim x$$

(which is a bijection) where $\sim$ denotes a group element acting on a set element, and $\forall x \in X$,
  - $e \sim x = x$
  - $(gh) \sim x = g \sim (h \sim x)$
- Equivalently, a function

$$\psi : G \to Sym(X)g \mapsto \phi_g$$

  - $$\ker\psi = \bigcap_{x \in X} G_x$$

    (intersection of all stabilizers)
- Interesting actions:

- Left multiplication of G on G:

$$\phi : G \to G \to G \qquad g \mapsto \phi_g : G \to G \qquad h \mapsto gh$$

  - $\mathcal{O}_x = G$ (transitive)
  - $G_x = e$
- G acting via conjugation on itself:

$$\phi : G \to G \to G \qquad g \mapsto \psi_g : G \to G \qquad h \mapsto ghg^{-1}$$

  - A common notation is $x^g = g^{-1}xg$ which obeys $(x^g)^h = x^{gh}$
  - $\mathcal{O}_x = [x]$ (Conjugacy classes, so not generally transitive)
  - $G_x = \{g \in G : gxg^{-1} = g\} = C_G(x)$
- G acting on $S = \{H : H \leq G\}$ via conjugation:
  - $$\phi : G \to S \to S \qquad g \mapsto \psi_g : S \to S \qquad H \mapsto gHg^{-1}$$
  - $\mathcal{O}_H = [H] = \{gHg^{-1} : g \in G\}$, conjugate subgroups of H
  - $G_x = N_G(H) = \{g \in G : gHg^{-1} = H\}$

2.1.9 Transitive group actions

- $\forall x, y \in X, \exists g \in G : g \sim x = y$
- Equivalent, actions with a single orbit

2.1.10 Orbit of a set element

$$\mathcal{O}_x = \{g \sim x : x \in X\text{ă}\} = \bigcup_{g \in G} \{g \sim x\}$$

- The set of all orbits is denoted X/G or $X_G = \{\mathcal{O}_x : x \in X\}$
- Partitions X according to the equivalence relation $x \cong y \iff \exists g \in G : g \sim x = y$
- G acts transitively on X when restricted to any single orbit

2.1.11 Stabilizer of a set element

- $G_x = \{g \in G : g \sim x = x\}$
- Facts:
  - $G_x \leq G$, not usually normal
  - $x, y \in \mathcal{O}_x \Rightarrow G_x$ is conjugate to G_y

2.1.12 Automorphisms of a group

- $Aut(G) = \{\phi : G \to G : \phi \text{ is an isomorphism}\}$

2.1.13 Inner Automorphisms of a group

- $Inn(G) = \{\phi_g \in Aut(G) : \phi_g(x) = gxg^{-1}\}$
- Also consider the map
$$\psi : G \to Aut(G) g \mapsto (\lambda : x \mapsto gxg^{-1})$$
  Then $\text{im}\psi = Inn(G), \ker\psi = Z(G)$
- Facts:
  - $Inn(G) \trianglelefteq Aut(G)$
  - $Inn(G) \cong G/Z(G)$

2.1.14 Outer Automorphisms of a group

- $Out(G) = Aut(G)/Inn(G)$

2.1.15 Conjugacy Class of an element

- $$[a] = \{gag^{-1} : g \in G\} = \bigcup_{g\in G} \{gag^{-1}\}$$
- Equivalently, $[a] = \mathcal{O}_a$ under G acting on itself via conjugation
- Facts:
  - Equivalence relation, partitions the group
  - $|[a]|$ divides $|G|$
  - $a \in Z(G) \Rightarrow [a] = \{a\}$

2.1.16 Characteristic subgroup

- H char $G \iff \forall\phi \in Aut(G), \phi(H) = H$
  - i.e., H is fixed by all automorphisms of G.

2.1.17 Simple group

- G is simple $\iff H \trianglelefteq G \Rightarrow H = e$ or G
  - No non-trivial normal subgroups

2.1.18 Commutator of an element, or of subgroups

- $[g, h] = ghg^{-1}h^{-1}$
- $[G, H] = \langle [g, h] : g \in G, h \in H\rangle$ (Subgroup generated by commutators)

2.2 Structural Results

- Cyclic $\Rightarrow$ abelian
- $G/Z(G)$ cyclic $\Rightarrow G$ is abelian
- Intersections of subgroups are also subgroups

2.2.1 Isomorphisms Theorems

-*First Isomorphism Theorem**

- Conditions:
  - $\phi : G \to G'$ is a homomorphism.
- Result:
  - $\ker\phi \trianglelefteq G$
  - $\text{im}\phi \leq G'$
  - $G/\ker\phi \cong \text{im}\phi$.
- Corollaries:
  - $\ker\phi = e \Rightarrow G \cong G'$

-*Second Isomorphism Theorem**

- Conditions:
  - $N \trianglelefteq G, H \leq G$
- Results:
  - $HN \leq G$
  - $N \bigcap H \trianglelefteq H$
  - $$\frac{H}{H \bigcap N} \cong \frac{HN}{N}$$
- Corrolaries:
  - (Weaker) Relaxing $N \trianglelefteq G$ to $H \subseteq N(N)$ yields
    - $N \bigcap H \subseteq G$ (Not normal)
    - $N \bigcap H \trianglelefteq H$

-*Third Isomorphism Theorem**

- Conditions:
  - $N \trianglelefteq G, N \leq A \leq G$
- Results:
  - $A/N \leq G/N$
    - Every subgroup of G/N is of this form for *some* such A
  - $$\frac{G/N}{A/N} \cong \frac{G}{A}$$
    - Cancel the N!
- Corrolaries:
  - $A \trianglelefteq G \Rightarrow A/N \trianglelefteq G/N$
    - All normal subgroups of G/N are of this form for some A.

2.3 Misc Results

- G/N is abelian $\iff [G, G] \leq N$
- HK is not always a subgroup - see conditions in 2nd Isomorphism theorem'
- $H \trianglelefteq G, K \trianglelefteq G$ and $H \bigcap K = e \Rightarrow hk = kh \forall h \in H, \in K$
  - Normal subgroups with trivial intersection commute
- H char $G \Rightarrow H \trianglelefteq G$

- Characteristic is a strictly stronger condition than normality
- H char K char $G \Rightarrow H$ char G
  - Characteristic is transitive
- $H \leq G$, $K \trianglelefteq G$, H char $K \Rightarrow H \trianglelefteq G$
  - i.e., normality is **not** transitive, strengthening normality to char gives "weak transitivity"
- Recognizing (Internal) Direct Products:$H \leq G, K \leq G$
  - $H \bigcap K = e$
  - $\forall g \in G, \exists h \in H, k \in K : g = hk$
  - $H \trianglelefteq G, K \trianglelefteq G$
    * **OR** Every element in H commutes with every element in K
- P Groups
  - $\bigcap P = O_P(G)$ char G. And $O_P(G) \trianglelefteq G$ as well.
  - $N \trianglelefteq G$ implies that $P_N \leq N$ are of the form $N \bigcap P_G$
  - $P \bigcap Q = e$

2.4 Numeric Results

2.4.1 Cauchy's Theorem

- For any p dividing $|G|$, there is a subgroup of order p.

2.4.2 Sylow Theorems: $|G| = p^k m$ where $p \not| m$

- At least one Sylow-p subgroup always exists: $\exists P \leq G$ with $|P| = p^k$
- All such subgroups are conjugate: $\forall P, P', \exists g \in G : gPg^{-1} = P'$
- n_p satisfies:
  - n_p divides $m = [G : P]$
  - $n_p = 1 \mod p$
  - $n_p = [G : N_G(P)]$ (Not as useful)
- Every p-subgroup of G is a p-subgroup of P (i.e. P is maximal and contains all subgroups of order p^l with $l \leq k$)

2.4.3 Orbit-stabilizer Theorem

- Given a group action, $G/G_x \cong \mathcal{O}_x$
- Gives the numeric result $|\mathcal{O}_x| = |G/G_x| = [G : G_x] = \frac{|G|}{|G_x|}$
- Also useful in the form $|G| = |\mathcal{O}_x||G_x|$
- Proof:
  - Use the map
$$\phi : G \to Xg \mapsto g \sim x$$
    Where im$\phi = \mathcal{O}_x$ and ker$\phi = G_x$.

2.4.4 Burnside's Lemma

- $$|X_G| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$
  - $|X_G|$ is the number of orbits
  - $X^g = \{x \in X : g \sim x = x\}$

2.4.5 The class equation

- $$|G| = |Z(G)| + \sum_{a\in A}[G : C_G(a)]$$
  - Where $A = \{a_1, a_2, \ldots, a_n : a_1 \in [a_1], a_2 \in [a_2], \ldots\}$ is a set containing one element from each conjugacy class
  - $[G : C_G(a)]$ is the number of elements in $[a]$
  - Each element in $Z(G)$ has a singleton conjugacy class

2.4.6 General facts

- $|G| = p \Rightarrow G$ is cyclic
- $|G| = p^e \Rightarrow Z(G) \neq e$
- $|G| = p^e$ (P-groups)
  - $Z(G) \neq \{e\}$ (Use class equation)
- $|G| = p$
  - Always cyclic
    - Proof: Any nontrivial cyclic subgroup's order is > 1 and divides p, so equals p.
- $|G| = p^2$
  - Always abelian
    - Proof: $|G/Z(G)| = 1, p$. If p, it's cyclic, and G is abelian. Otherwise it's 1, so $G = Z(G)$.
  - Two possibilities:
    - Z_{p^2} (cyclic)
    - $Z_p \times Z_p$
- $|G| = pq$
  - $p \not\Big| \; q - 1 (q \neq 1 \mod p)$:
    - One possibility:
      - $G \cong Z_{pq}$ (cyclic)
    - Facts:
      - $\exists P \trianglelefteq G$ (A Sylow-P subgroup)
  - p divides $q - 1$ ($q = 1$ mod p):
    - Two possibilities:

        - $G \cong Z_{pq}$ (cyclic)
        - $G \cong Z_q \rtimes Z_p$
    - Never simple
- $|G| = p^2q$
    - $\exists P \trianglelefteq G$ (A Sylow-P subgroup)
- $|G| = p_1p_2p_3$ (distinct)
    - Not simple

2.5 Common Groups

2.5.1 S_3

$S_3 = \langle (12), (23), (13) \rangle$

- $Z(S_3) = e$
- $Aut(S_3) = Inn(S_3)$, since

$$Z(G) = e = \ker\psi \Rightarrow Out(S_3) = Inn(S_3) \Rightarrow Aut(S_3) \cong S_3$$

2.5.2 S_n

$S_n, n \geq 4$

- $Z(S_n) = e$
    - Let $\sigma(a) = b$, choose $\tau = (bc)$ so $\tau\sigma(a) = \tau(b) = c \neq b = \sigma(a0 = \sigma\tau(a)$
- Conjugacy classes are determined entirely by cycle structure
    - There are exactly $p(n)$ of them (partition function)
- Disjoint cycles commute
- $\sigma \circ (a_1 \cdots a_k) \circ \sigma^{-1} = (\sigma(a_1), \cdots \sigma(a_k))$
- Every element is a product of disjoint cycles
- Every element is a product of transpositions
    - A cycle of length k can be written as $k - 1$ transpositions
    - Parity of the cycle equals the parity of $k - 1$.
- The order of an element is the lcm of the size of the cycles.

2.5.3 A_n

- Simple for $n \geq 5$
- Index 2 in S_n, so $A_n \trianglelefteq Sn$

2.5.4 D_n

- $\langle a, b \mid a^n = b^2 = 1, bab^{-1} = a^{-1} \rangle \cong \langle r, s \rangle$
- D_n/N is always another dihedral group for any $N \trianglelefteq D_n$
- All subgroups:
    - $\langle r^d \rangle \cong Z_{n/d}$ where d divides n (index $2d$)
    - $\langle r^d, r^i s \rangle \cong D_{\frac{n}{d}}$ where d divides n and $0 \leq i \leq d - 1$ (index d)

* All dihedral

3 Rings

3.1 Facts about ideals:

- Intersections, products, and sums of ideals are ideals
- Not necessarily unions
- Every ring has proper maximal ideals
- Apply Z.L. to $\{I \trianglelefteq R : I \neq R\}$
- Every proper ideal is contained in a maximal ideal

3.2 Maximal ideals

$I \trianglelefteq R$ *maximal* if $\nexists J \trianglelefteq R : I \subset J \subset R$

- Every nonzero ring has a maximal ideal (Krull's Theorem)
- R commutative $\implies R/I$ a field
- Union of maximal ideals $= R - R^{\times}$
- $(X - a) \trianglelefteq R[X]$ is maximal for $a \in R$

3.3 Prime ideals

$I \trianglelefteq R$ *prime* when $pq \in I \implies p \in I \vee q \in I$

- I prime $\iff R/I$ an integral domain,
- (maximal $\implies$ prime)
- $\operatorname{rad}(I^n) = I$

3.4 Radicals

$I \trianglelefteq R$ *radical* when $\forall a \in R, a^n \in I \implies a \in I$

- The nilradical: $\operatorname{nilrad}(I) = \bigcap P$ such that $P \trianglelefteq R$ is prime
- $\operatorname{rad}(I) = \{x \in \mid \exists n : x^n \in I\}$
- $\operatorname{rad}(0) = \operatorname{nilrad}(R)$
- $\operatorname{rad}(IJ) = \operatorname{rad}(I) \bigcap \operatorname{rad}(J)$
- $\operatorname{rad}(I) = \bigcap J$ such that $I \subset J, J$ prime (i.e. intersection of all prime ideals containing I)

3.5 Other ideals

- $I \trianglelefteq R$ *primary* when $pq \in I \implies a \in I \vee \exists n \in \mathbb{N} : b^n \in I$
- Prime $\implies$ primary
- $I \trianglelefteq R$ *principal* when $\exists a \in R : I = \langle a \rangle$
- $I \trianglelefteq R$ *irreducible* when $\nexists \{J \trianglelefteq R : I \subset J\} : I = \bigcap J$

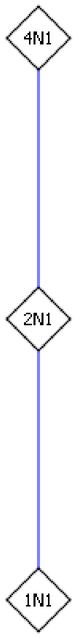
- $I \subset R \iff 1, u \notin I$ $(u \in R^\times)$
- $\{I : I \trianglelefteq R\}$ is a poset
- Zorn's lemma can be applied to $\{I \trianglelefteq R : 1 \notin I\}$
- Every proper ideal is contained in a maximal ideal.
- Facts about units
- $R^\times$ is closed under multiplication, but *not* under addition.
- $R - R^\times$ an additive group $\iff$ R is a local ring
- Integral Domain
- Principal Ideal Domain
- (Prime $\implies$ maximal) $\implies$ UFD
- Unique Factorization Domain
- Field
- When (0) is the only proper ideal
- R/M a field $\iff$ M maximal
- Localization
- Zorn's Lemma: For every poset P, every chain in P has an upper bound $\implies$ P has a maximal element.
- Noetherian: Every ideal is finitely generated
- iff the ascending chain condition for ideals holds

3.6 Orders less than 16:

(Normal: Diamond, grouped by conjugacy class)

- 1 (The trivial group)
  - $Z_1 = \{e\}$
- 2 (One group)
  - $Z_2 \cong Z_3^\times \cong Z_4^\times \cong Z_6^\times$
    $= \{e, a\}$
    * Cyclic
    * One element of order 2
- 3 (One group)
  - $Z_3 \cong A_3$
    $\cong \{(), (123), 132)\}$
    * Cyclic
    * One element of order 3

- 4 *(Two groups, both abelian)*
  - $Z_4 \cong Z_5^\times \cong Z_8^\times \cong Z_{10}^\times \cong Z_{12}^\times$
    - Cyclic
    - One element of order 4
  - $Z_2 \times Z_2 \cong V_4 \cong D_2 \cong Z_8^\times$
    $\cong \langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle$
    $\cong \langle (12)(34), (13)(24), (14)(23) \rangle$
    - Not cyclic, but abelian
    - All elements have order 2
    - $V_4 \trianglelefteq A_4 \leq S_4$



  -

- 5 (One group)
  - Z_5
    - Cyclic, one element of order 5
- 6 *(Two groups)*
  - $Z_6 \cong Z_7^\times \cong Z_9^\times \cong Z_{14}^\times$
    - Cyclic, one element of order 6
  - $S_3 \cong D_6$
    $\cong \langle a, b, c \mid a^2 = b^2 = c^3 = abc = e \rangle$
    - Non-abelian (smallest one)
    -

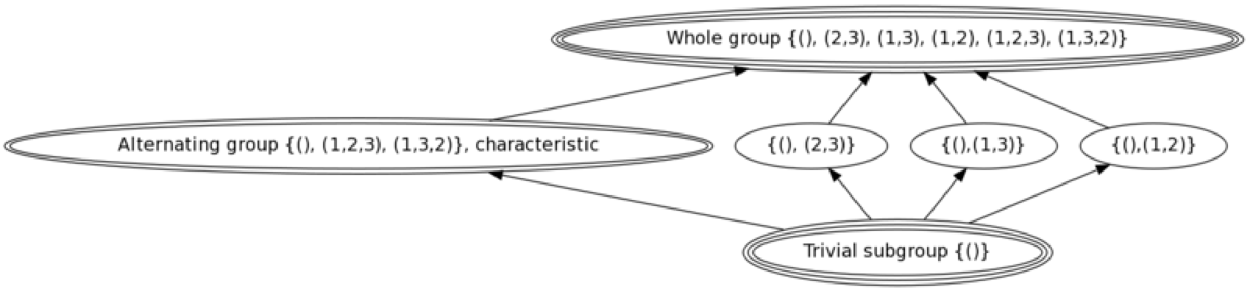


Figure 1: File:S3latticeofsubgroups.png

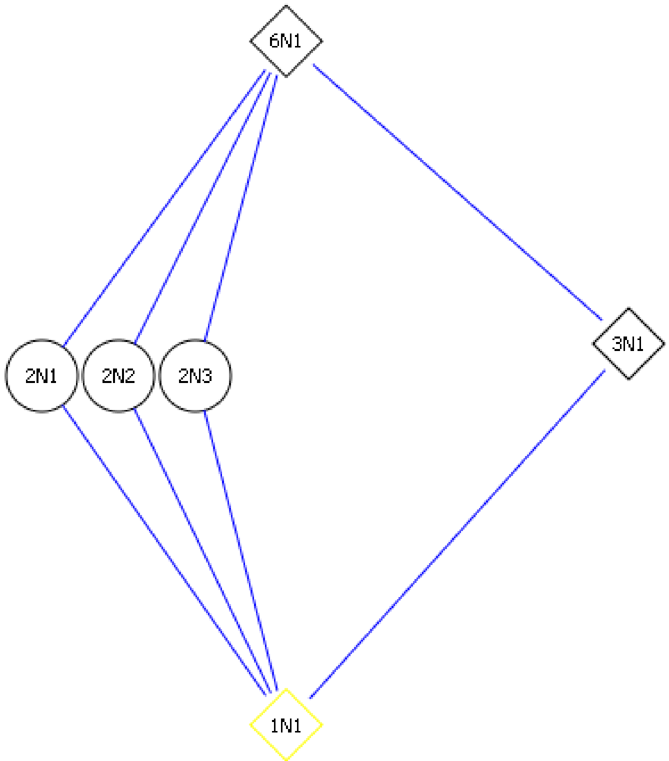
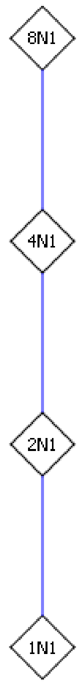


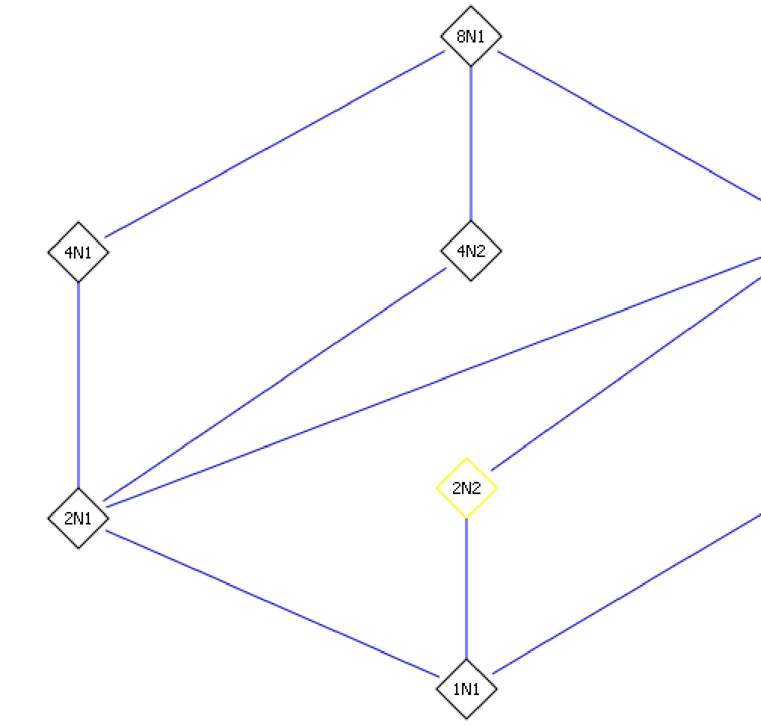
Figure 2: img

    *

- 7 (One group)
  - Z_7
    * Cyclic, one element of order 7
- 8 **(Five groups)**

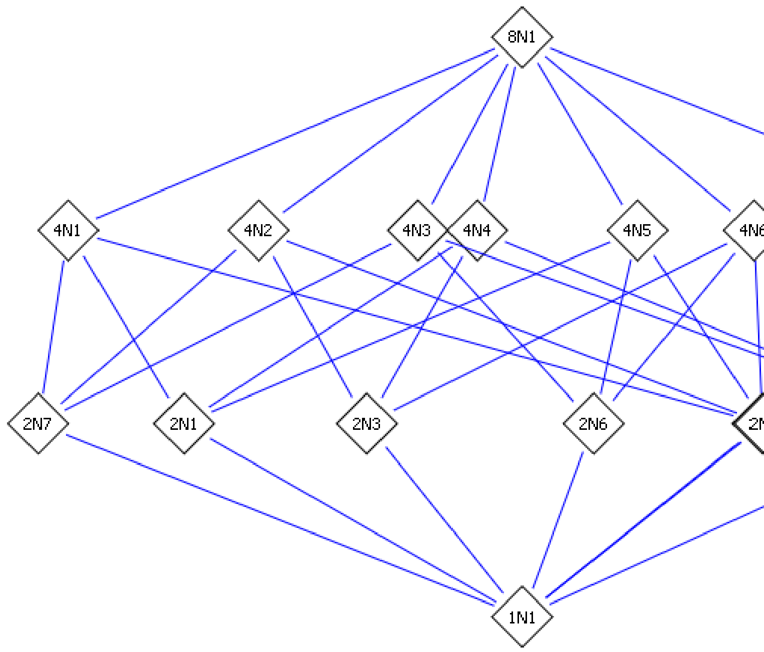


  - $Z_8 \cong Z_{15}^{\times} \cong Z_{16}^{\times}$ (cyclic)
  - $Z_2 \times Z_4$



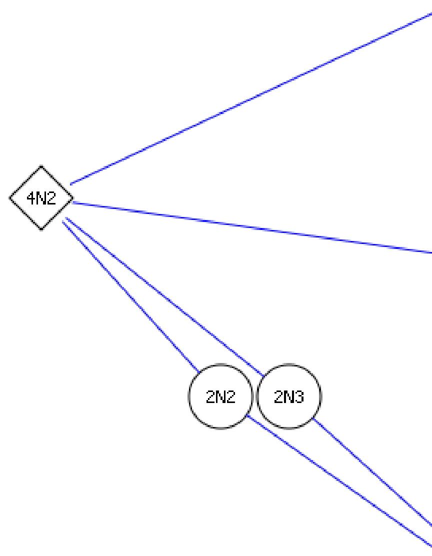
* Abelian, one element of order 4

- $Z_2 \times Z_2 \times Z_2$



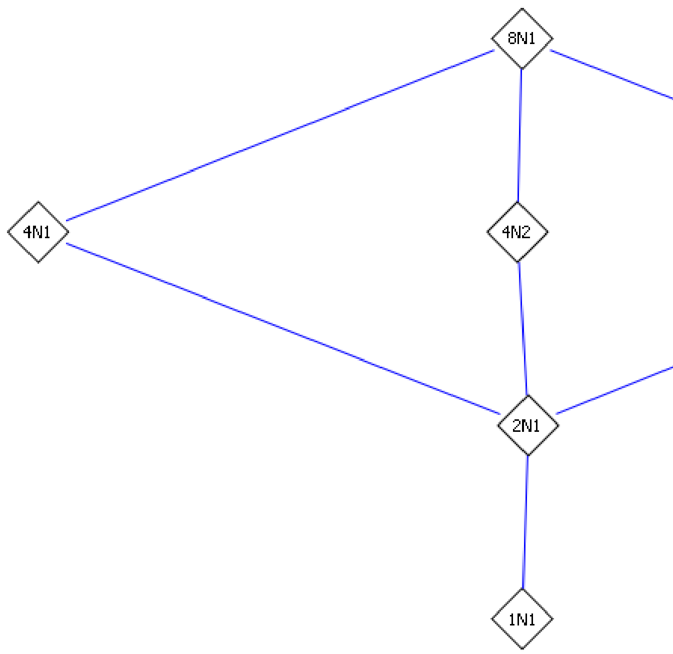
* Abelian, every element has order 2

- $D_8 \cong \langle r, s \mid r^4 = s^2 = e, srs^{-1} = r^{-1} \rangle$



$\cong \{(), (1234), (13)(24), (1432), (13)(24), (14)(23), (12)(34)\} \leq S_4$

- $Q_8 \cong \langle i, j, k \mid i^2 = j^2 = k^2 = ijk \rangle$
  $\cong \langle a, b, c \mid a^4 = b^4 = e, a^2 = b^2, ba = a^3 b \rangle$
  * Every element has order 4



  * All subgroups are normal, but not abelian

- 9 *(Two groups)*
  - Z_9
  - $Z_3 \times Z_3$
- 10 *(Two groups)*
  - $Z_{10} \cong Z_{11}^{\times}$
  - D_{10}
- 11 (One group)
  - Z_{11}
- 12 **(Five groups)**
  - $Z_{12} \cong Z_{13}^{\times}$
- 13 (One group)
  - Z_{13}
- 14 *(Two groups)*
  - Z_{14}
- 15 (One group)
  - Z_{15}
- 16 ***(Fourteen groups!)***